DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE
EQUIPAMENTOS
DE INFORMÁTICA
INCLUINDO
ASSISTÊNCIA
TÉCNICA E
TREINAMENTO

HP INVENT –
MANUAL
APÊNDICES DT A
DZ

2003
PASTA 09

Apêndice DT

5814

A4902A- HP Rack System/E, 41U, 19" quartz
A4902D- HP Rack System/E, 41U, 19" graphite ■

Technical Data

Save valuable floor space with the vertically extendible HP Rack System/E

Designed and built to the highest HP quality standards, the Rack System/E delivers leading edge protection in the simplest form. Ease of use, integration and installation characterizes this 41U rack that is comprised of:

- 63% Perforated, locking rear door (ordered as A5213AZ/A5213DZ)
- Bolt-on front/back anti-tip feet
- Numbered columns
- Fully perforated top cap
- 3-inch urethane casters
- Leveling feet
- Side panels

Multiple racks may be tied together to create continuous data center rack space. Individual racks may be expanded an additional 8Us of vertical space.

Standards

Conforms to the Electronic Industries Association (EIA) standard 310-D. It is a Type A cabinet with 41U of vertical mounting space. One 'U' is equal to 44.45 mm (1.75 in).

Customer must order rear door, A5213AZ(quartz)

A5213DZ (graphite)

Features

- Ability to move and ship fully integrated racks
- Optimized ventilation with fully perforated top, and rear door
- Extendibility can add 8Us of vertical mounting space
- Easy, bolt-on (front and back) anti-tip feet
- Numbered 12-gauge steel columns for easy installation and secure racking of up to 907 kg (2000 lbs) of equipment
- Columns include threaded inserts (AVKs) at strategic locations for quick installation of common accessories such as the tie kit, front door and PDUs

Shipping/Setup

- Can fit through most doorways around the world
- Packaging designed for integrated rack shipment
- Self-tuning pallet adjusts for variable integrated rack weights
- Shipping pallet includes ramp for easy set-up

Product Number
A4902D

Tools required for setup:

- Torx T25 screwdriver
- Phillips #2 screwdriver
- 13mm Socket wrench

Warranty

One- year replacement

Specifications

Color (A4902A- quartz)
Columns and base: Slate gray
Top: Quartz gray
Side panels: Quartz gray
Rear door: Quartz gray

Color (A4902D- graphite)
Columns and base: Graphite metallic
Top: Graphite metallic
Side panels: Graphite
Rear door: Graphite metallic

Material
Columns: 12-gauge, cold-rolled steel
Base: 10-gauge, cold-rolled steel
Top cap: 18-gauge, cold-rolled steel

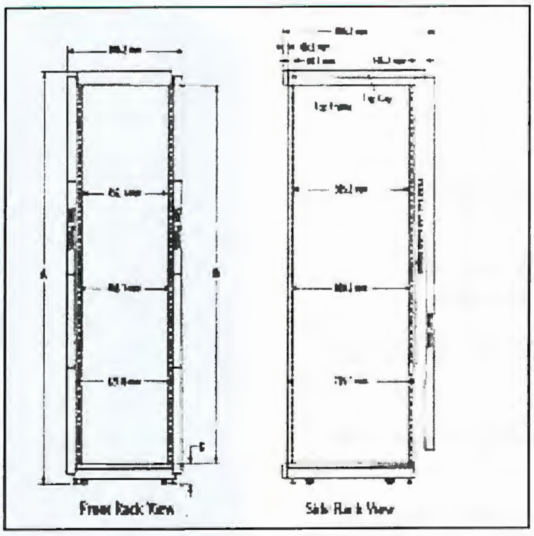
583

A4902D

A	1961.1 mm
B	1824.7 mm
C	111.2 mm

A4901D

A	1605.5 mm
B	1469.1 mm
C	111.2 mm



Weight
Rack (empty): 100.45 kg (221 lbs)
Rack (empty) on shipping pallet: 169.3 kg (372.5 lbs)
Rear door (unpacked): 10.68 kg (23.5 lbs)
Anti-tip foot: 16.14 kg (35.5 lbs)

Supported weight
Load capacity:
On shipping pallet: 816 kg (1800 lbs);
Off shipping pallet: 907 kg (2000 lbs)
Casters rating: 453.6 kg (1000 lbs) per caster

* Dimensions are for reference only

Related Products

Other sizes available are:

- **A4901A (quartz)**
- **A4901D (graphite)**
  - 33U of vertical mounting space, includes side panels, bolt-on (front and back) anti-tip feet
- **A4900A (quartz)**
  - 25U of vertical mounting space,includes side

Profundidade - 742 mm

Optional Accessories

J1506A/ J1506D	Side Panel Kit (1 kit per rack) included in standard rack
J1509A/ J1509D	Front Door: Perforated, lockable
J1512A/ J1512D	Tie Kit
J1514A/ J4387A	Filler Panels (set of 6)
J1518A/ J1518D	Keyboard Kit, retractable
J1519A/ J1519D	Monitor Kit
J1520A/ J1520D	Plain Shelf, static
J1521A	Lift Hooks (set of 4)
J1522A	Mounting Hardware

Apêndice DU

hp-ux 11i
oes

hp-ux 11i operating environments
enterprise release

hp-ux 11i
oes

hp-ux 11i operating environments benefits

greatly simplified software deployment

- Only one reboot needed to install the Operating Environment (OE) of your choice
- No codewords are necessary to access any of the functionality/application products resident on the OE media
- Comprehensive offering of Network, Mass Storage, and I/O Drivers available during install process
- Online Diagnostics loaded during cold install

simple to purchase license

- Each OE license product contains licensing for the base HP-UX O/S and all of the included HP applications

attractive pricing

- Pricing of the OE licenses reflects a built-in advantage over purchasing individual OE components separately

published testing results

- Testing results of application products in the OEs will be published on docs.hp.com for worldwide access both inside and outside HP

simple to purchase software support

- Simplification in Software Support ordering and contract administration has been achieved in parallel with the introduction of HP-UX 11i Operating Environments
- For more information, please visit: http://nternet.fc.hp.com/catscore/communic.htm

hp-ux 11i
oes

getting to know hp-ux operating environments

- The following series of slides will show how HP-UX 11i Operating Environments are constructed from pieces of the total 11i Software Solution

3810

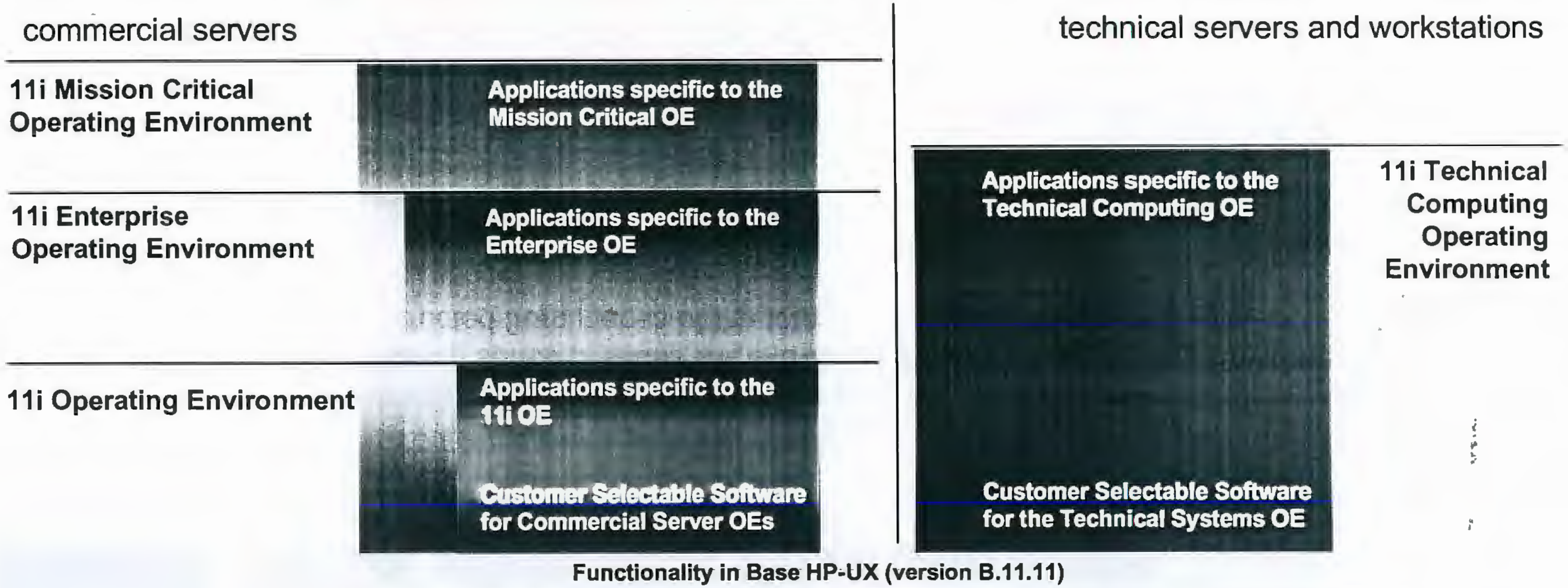
hp-ux 11i
oes

getting to know hp-ux operating environments

5809

design overview

- Each of the Commercial Server Operating Environment license and media products are designed to be supersets of one another
- The TCOE represents a singular solution for Technical Servers and Workstations
- Base HP-UX and Application content common across all four OEs is synchronized with the same revision level



commercial servers

technical servers and workstations

11i Mission Critical Operating Environment

Applications specific to the Mission Critical OE

11i Enterprise Operating Environment

Applications specific to the Enterprise OE

11i Operating Environment

Applications specific to the 11i OE

Customer Selectable Software for Commercial Server OEs

11i Technical Computing Operating Environment

Applications specific to the Technical Computing OE

Customer Selectable Software for the Technical Systems OE

Functionality in Base HP-UX (version B.11.11)

hp-ux 11i
oes

getting to know hp-ux operating environments

- HP-UX version B.11.11 is at the heart of each HP-UX 11i Operating Environment and provides the sound foundation onto which each OE Solution is built
- Two global base HP-UX bundles are delivered at B.11.11 and are differentiated by bitness: HPUXBase64 for 64-bit capable hardware, and HPUXBase32 for 32-bit capable hardware

HP-UX 11i Core Functionality
HPUXBase64 (64-bit)
HPUXBase32 (32-bit)

5808

11i (B.11.11) operating system features

major new features of hp-ux 11i (version B.11.11 and future)

- Built-in Unlimited Simultaneous User Level License for HP-UX
- Includes Linux APIs
- Introduces online replacement and addition of I/O cards for N-Class and L-Class servers
- Fully supports the low-end A500 and A400 servers, designed for ISP operation, where performance per rack and serviceability are keys
- Supports L2000 and L1000, an economical N-Class server with an upgrade path to IA-64
- Supports the V2500/V2600 platform
- Offers VERITAS (JFS 3.3) file system support
- Has improved and expanded file system support from CacheFS
- Supports NFS over TCP/IP
- Adds systems management improvements (PRM enhancements)
- Offers secure defaults and intrusion detection
- Has extensive performance tuning for one-way to 32-way configurations

more information on the www

- HP-UX 11i Quick Reference Card
  http://esp.cup.hp.com:2000/nav24/ppos/358/hPUX/11iQRC.pdf

- 11i Technical Overview paper on ESP
  http://esp.cup.hp.com:2000/nav24/ppos/358/hPUX/technOverv/techOV.doc

Apêndice DV

QuickSpecs

HP Smart Array 641 Controller
HP Smart Array 642 Controller
HP 64MB BBWC Enabler

Standard Features

The Smart Array Advantage

HP's innovative design and integration work of the Smart Array family of products creates customer value that is unmatched in the industry. Use of Smart Array products across multiple applications results in a much lower Total Cost of Ownership (TCO) than any other server storage RAID products. The HP Smart Array family brings an unparalleled return on investment through:

Data Compatibility	Data Compatibility among all models of Smart Array controllers allows simple and easy upgrades any time needs for higher performance, capacity, and availability increase. Even successive generations of Smart Array controllers understand the data format of other Smart Array Controllers.
Consistent Configuration and Management Tools	All Smart Array products utilize a standard set of management and utility software. These tools minimize Total Cost of Ownership (TCO) by reducing training requirements and technical expertise necessary to install and maintain the HP server storage.
Universal Hard Drive	Form factor is for use across multiple HP ProLiant servers, disk enclosures and storage systems. With compatibility across many enterprise platforms, you are free to deploy and re-deploy these drives to quickly deliver increased storage capacity, migrate data between systems, and easily manage spare drives.
Pre-Failure Warranty	Pre-Failure Warranty means Insight Manager not only reports when a drive is going to fail but allows replacement of failing drives prior to actual failure. For complete details, consult the HP Support Center or refer to your HP Server documentation.

Key Features for both Smart Array 641 and Smart Array 642 Controllers

- Compatibility with all Ultra 320, Ultra3 and Ultra2 LVD family products. In addition, a seamless upgrade to next generation HP high performance and high capacity mainstream Ultra320 Smart Array controllers.
- Recovery ROM protects against a ROM corruption.
- Ultra320 SCSI technology delivers high performance and data bandwidth up to 320-MB/s bandwidth per channel.
- Modular, easy-to-upgrade design lets you optimize performance as needed with the 64MB BBWC Enabler, from 64-MB of memory for RAID and read cache to 128-MB of memory for RAID, read cache, and BBWC.
- Mix-and-match LVD SCSI compatibility protects your investments and lets you deploy drives as needed.
- Software consistency among all Smart Array family products: Array Configuration Utility XE (ACU-XE), Array Configuration Utility (ACU), Insight Manager (CIM), Array Diagnostic Utility (ADU) and SmartStart.
- 64-bit, 133-MHz PCI-X interface boosts bandwidth above 1B/s burst transfer rate over PCI-X bus.
- 64-bit memory addressing supports servers with greater than 4 GB of memory.
- 64-MB memory optimizes performance and data throughput.

NOTE: 64 MB of DDR memory used for RAID and read cache.

Online Management Features	Online Capacity Expansion, Online RAID Level Migration, Online Stripe Size Migration, Online Spares (Global), User Selectable Expand and Rebuild Priority
Channels	▪ **SA 641 : Single Channel** provide the ability to support up to 6 drives or 880.8GB ▪ **SA 642 : Dual Channels** provide the ability to support up to 20 (6 internal, 14 external) drives or 2.9TB

Key Features for 64MB BBWC Enabler

- Battery-backed Cache protects cached data in the event of a power outage, server failure or controller failure.
- 72 hours of battery charge protects the data for an entire weekend.
- 3 years of battery life.
- Modular, easy-to-upgrade design lets you optimize performance as needed with the 64MB BBWC Enabler, from 64-MB of memory for RAID and read cache to 128-MB of memory for RAID, read cache, and BBWC.

Data Compatibility

Data compatibility among all models of Smart Array Controllers means customers can instantly upgrade their Smart Array products to get to higher performance, capacity and availability. Unlike competitive products, successive generations of Smart Array products understand the data format of other Smart Array controllers, providing investment protection for your HP storage solution.

QuickSpecs

S806

HP Smart Array 641 Controller
HP Smart Array 642 Controller
HP 64MB BBWC Enabler

Overview

Smart Array 641 Controller

The new Smart Array 641 Controller (SA-641) is a 64-bit, 133-MHz PCI -X dual SCSI channel PCI array controller for entry level hardware-based fault tolerance. Utilizing a SCSI channel (1 internal) of the SA-641 allows you to configure up to 6 internal hard drives to store up to 880.8 GB of storage. The SA-641 provides high reliability and increased performance over the LC2 controller, thus providing excellent value and lowering the total server ownership cost. In addition, the SA-641 is data compatible with all Ultra 320, Wide Ultra3 and Wide Ultra2 drives, offering an unparalleled degree of investment protection. Designed and integrated with HP entry-level and workgroup ProLiant servers, this product provides worry-free data protection.

Smart Array 642 Controller

The new Smart Array 642 Controller (SA-642) is a 64-bit, 133 MHz PCI-X dual SCSI channel PCI array controller for entry level hardware-based fault tolerance. Utilizing both SCSI channels (1 internal and 1 external) of the SA-642 allows you to configure up to 20 hard drives (6 internal, 14 external) to store up to 2.9TB of storage per PCI slot. The SA-642 provides high reliability and increased performance over the Smart Array 532, thus providing excellent value and lowering the total server ownership cost. In addition, the SA-642 is data compatible with all Ultra 320, Wide Ultra3 and Wide Ultra2 drives, offering an unparalleled degree of investment protection. Designed and integrated with HP entry-level and workgroup ProLiant servers, this product provides worry-free data protection.

The Smart Array 641/642 Controller provides ProLiant DL and ML servers with an entry-level hardware RAID protection for OS and log files, where hardware RAID is needed at an entry-level price point.

64-MB BBWC (Battery-Backed Write Cache) **Enabler**

The new 64MB BBWC Enabler is a transportable 64MB battery module increasing the total memory of the controller to 128MB for RAID, read cache, and BBWC. The transportability of the battery memory module protects the write cache data from unexpected power loss, system board failure, or controller board failure. Data retained in the write cache will be protected for up to 72 hours, allowing time to restore power, or transport the module to a functioning system board or array controller. The modular design of the battery memory module is transportable between the Smart Array 641 and Smart Array 642 controllers.

64MB BBWC (Battery Backed Write Cache) Enabler allows the 641/642 controllers an option to add transportable BBWC for improved controller performance and increases the total controller memory to 128MB.

invent

Standard Features

Ease of Use

Consistency and Upgradeability make the Smart Array family unique in the industry:

- GUI based configuration, management and diagnostic software tools
- Common data formatting between generations of products
- Data migration between servers and external storage enclosures

Compatibility

Servers

For up to date compatibility, please see the following URL for complete Smart Array 641 and Smart Array 642 compatibility and support information. http://h18006.www1.hp.com/products/servers/proliantstorage/arraycontrollers/index.html

Operating Systems

5803

Microsoft® Windows® 2000 (Server/Adv Server)
Microsoft Windows 2003 (when available)
Microsoft Windows NT® 4.0
NetWare 6
NetWare 5.x
Linux Red Hat 2.1 Advanced Server
Linux Red Hat 7.3
Linux Red Hat 8.0
SuSE SLES 7
IBM OS/2 Warp Server for ebusiness
SCO Open Server 5.05, 5.0.7 (to be released 1Q, 03)
SCO UnixWare 7.1.1
SCO Open UNIX® 8
SCO UnixWare 7.1.3 (to be released 4Q, 02)

Software Suite

All Smart Array products share a common set of configuration, management and diagnostic tools, including Array Configuration Utility XE (ACU-XE), Array Configuration Utility (ACU), Array Diagnostic Utility (ADU), and Insight Manager. This software consistency of tools reduces the cost of training for each successive generation of product and takes much of the guesswork out of troubleshooting field problems. These tools lower the total cost of ownership by reducing training and technical expertise necessary to install and maintain the HP server storage.

Insight Manager

- Powerful server and server options/storage manager tool
- Monitors over 1200 server parameters
- Configuration/Diagnostic Utilities
- HP Array Configuration Utility (ACU)
  - Powerful Web based configuration utility for all Smart Array controllers
  - Provides a graphical view of HP drive array configurations
  - Allows for management of multiple arrays over a secure internet connection from anywhere in the world
  - Easy to use Wizards for configuration
  - Runs online on Windows NT v4.0, Windows 2000 and NetWare
- HP Options ROM Configuration for Arrays (ORCA)
  - Rapid configuration during initial install of the OS
- HP Array Diagnostic Utility (ADU)
  - Powerful diagnostic utility for all Smart Array controllers

S804

Standard Features

Performance

HP's High Performance Architecture sets new boundaries of industry performance expectations!

- Wide Ultra320 SCSI (320 MB/s bandwidth) per channel
- High-performance 64-bit architecture
- 64-bit, 133-MHz PCI-X bus (1033 MB/s bandwidth)

Capacity

Smart Array 641	Given the internal server storage need for rapid capacity expansion, the SA-641 offers: • Single SCSI channel support up to 6 internal disk drives • Up to 880.8GB of storage per PCI slot
Smart Array 642	Given the internal server storage need for rapid capacity expansion, the SA-642 offers: • Dual SCSI channels support up to 20 (6 internal, 14 external) disk drives • Up to 2.9 TB of storage per PCI slot

Availability

Provides increased server uptime by providing advanced storage functionality:

- Online RAID Level Migration (between any RAID level)
- Online Capacity Expansion
- Logical Drive Capacity Extension
- Global Online Spare
- Pre-Failure Warranty

Fault Prevention

The following features offer detection of possible failures before they occur, allowing preventive action to be taken:

- S.M.A.R.T.: Self Monitoring Analysis and Reporting Technology first developed at HP detects possible hard disk failure before it occurs, allowing replacement of the component before failure occurs.
- Drive Parameter Tracking monitors drive operational parameters, predicting failure and notifying the administrator.
- Dynamic Sector Repairing continually performs background surface scans on the hard disk drives during inactive periods and automatically remaps bad sectors, ensuring data integrity.
- Smart Array Cache Tracking monitors integrity of controller cache, allowing pre-failure preventative maintenance.
- Environment Tracking for External Storage System: Monitors fan speed and cabinet temperature of ProLiant Storage System and newer HP storage enclosures.

Fault Tolerance

Keeps data available and server running while a failed drive is being replaced; several fault tolerance configurations are supported including:

Distributed Data Guarding (RAID 5)	This allocates parity data across multiple drives and allows simultaneous write operations. It is recommended for up to 14 hard drives.
Drive Mirroring (RAID 1, 1+0)	This allocates half of the drive array to data and the other half to mirrored data, providing two copies of every file. It is a high-performance RAID.

Fault Recovery

Minimizes downtime, reconstructs data, and facilitates a quick recovery from drive failure.

Recovery ROM	Recovery ROM provides a unique redundancy feature that protects from a ROM image corruption. A new version of firmware can be flashed to the ROM while the controller maintains the last known working version of firmware. If the firmware becomes corrupt, the controller will revert back to the previous version of firmware and continue operating. This reduces the risk of flashing firmware to the controller.
On-Line Spares	Up to two spare drives can be installed prior to drive failure. If a failure occurs, recovery begins with an On-Line Spare and data is reconstructed automatically.

NOTE: On-Line Spares can only be used with RAID level 1, 1+0, and 5.

Service & Support, CarePaq and Warranty Information

Software Product Services

- Standalone telephone support
- Rights to new license version
- Media and documentation updates

580

Hardware Product Services

- Installation services
- On-site maintenance (includes warranty support)
- Response time upgrades during the warranty period
- Post-warranty coverage
- RAID setup and performance consulting via statement of work

For additional hardware installation and maintenance information, please refer to the URLs listed below:
http://www.compaq.com/services/carepaq/us/install/
http://www.compaq.com/services/carepaq/us/hardware/

Warranty Upgrade Options

- Response - Upgrade on-site response from next business day to same day 4 hours
- Coverage - Extend hours of coverage from 9 hours x 5 days to 24 hours x 7 days
- Duration - Select duration of coverage for a period of 1, 3, or 5 years

CarePaq Information

Sample part numbers:

3 years, uplift to 5 x 9, Next Day Response	FM-**XHW-36
3 years, uplift to 5 x 9, 4-hour Response	FM-**4HR-36
3 years, uplift to 7 x 24, 4-hour Response	FM-**724-36

NOTE: ** represents a two digit product specific code.

- CarePaq is defined as an upgrade to the product warranty attribute, available for a specific duration and hours of coverage.
- CarePaq is not available for less than the product's warranty duration.
- CarePaq is available for sale anytime during the warranty period for most products, but the commencement date will be the same as the Warranty Start Date (delivery date to end user customer). Proof of purchase may be required.
- CarePaq services are prepaid.

For additional CarePaq (hardware & software) information, as well as orderable part numbers, please refer to the URL listed below:
http://www.compaq.com/services/carepaq/index.html

S802

Models

Models	Smart Array 641 Controller	291966-B21
	Features	
	Single SCSI channel (1 internal)	
	ProLiant Integration	
	Reliability	
	Ultra320 SCSI	
	64-MB memory for code, transfer buffers and read cache	
	64-bit Architecture	
	64-bit/133-Mhz PCI-X Bus Design	
	Online Capacity Expansion	
	Online RAID level Migration	
	Smart Array 642 Controller	291967-B21
	Features	
	Dual SCSI channels (1 internal/1 external)	
	ProLiant Integration	
	Reliability	
	Ultra320 SCSI	
	64-MB memory for code, transfer buffers and read cache	
	64-bit Architecture	
	64-bit/133-Mhz PCI-X Bus Design	
	Online Capacity Expansion	
	Online RAID level Migration	
	64MB BBWC Enabler	291969-B21
	Features	
	64 MB battery/memory module for a total of 128MB of memory for RAID, read cache and battery backed write cache (BBWC)	
	72 hours of battery charge	
	3 year battery life	

Options

Storage Enclosures	Compaq StorageWorks Enclosure Model 4314T	190210-001
	Compaq StorageWorks Enclosure Model 4314R	190209-001
	Compaq StorageWorks Enclosure Model 4354R	190211-001
Related Products	Compaq RAID LC2 Controller	188044-B21
	Compaq Smart Array 5302/32 Controller	166207-B21
	Compaq Smart Array 5302/64 Controller	124992-B21
	Compaq Smart Array 5304/128 Controller	158939-B21
	Compaq Smart Array 5302/128 Controller	283552-B21
	Compaq Smart Array 5304/256 Controller	283551-B21

5800

Options

Hard Drives

Wide Ultra3 SCSI Universal Drives – Hot Plug

36.4-GB Wide Ultra3 SCSI 15,000 rpm Drive (1″)	232916-B22
18.2-GB Wide Ultra3 SCSI 15,000 rpm Drive (1″)	188122-B22
9.1-GB Wide Ultra3 SCSI 15,000 rpm Drive (1″)	188120-B22
72.8-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	232432-B22
36.4-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	176496-B22
18.2-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	142673-B22
9.1-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	142671-B22
36-GB Wide Ultra3 SCSI 10,000 rpm Drives (1″), 10 pack	232617-B21
18-GB Wide Ultra3 SCSI 10,000 rpm Drives (1″), 10 pack	202352-B21

Wide Ultra320 SCSI Drives –Hot Plug

146.8-GB 10,000 rpm U320 Universal Hard Drive (1″)	286716-B22
72.8-GB 10,000 rpm U320 Universal Hard Drive (1″)	286714-B22
36.4-GB 10,000 rpm U320 Universal Hard Drive (1″)	286713-B22
72.8-GB 15,000 rpm U320 Universal Hard Drive (1″)	286778-B22
36.4-GB 15,000 rpm U320 Universal Hard Drive (1″)	286776-B22
18.2-GB 15,000 rpm U320 Universal Hard Drive (1″)	286775-B22

Wide Ultra3 SCSI Drives – Non-Hot Plug

36.4-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	176497-B21
18.2-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	142674-B21
9.1-GB Wide Ultra3 SCSI 10,000 rpm Drive (1″)	142672-B21

Wide Ultra320 – Universal Non-Hot Plug

36-GB U320 10,000 rpm Non-Hot Plug Hard Drive (1″)	271832-B21

NOTE: This is a list of supported hard disk drives **(note that some drives may be discontinued)**.

Software

StorageWorks Virtual Replicator

License & Media (CD-ROM)	191802-B21

NOTE: For additional Virtual Replicator ordering information refer to http://www.compaq.com/products/StorageWorks/swvr/swvrorderinfo.html.

Universal Hot Plug Tape Drives

AIT 50 GB, Hot Plug (Carbon)	215487-B21
AIT 35 GB, LVD Hot Plug (Carbon)	216886-B21
20/40-GB, DAT Hot Plug (Carbon)	215488-B21

Technical Specifications

Smart Array 642

Protocol	Ultra320 SCSI
SCSI Electrical Interface	Low Voltage Differential (LVD)
Drives Supported	Up to 20 (6 internal and 14 external) Ultra 320, Ultra3 and Ultra2 SCSI hard drives
SCSI Port Connectors SA-642	One external and one internal SCSI port
Data Transfer Method	64-Bit PCI bus-master
PCI Bus Speed	64-bit, 133-MHz PCI-X (1 GB/s maximum bandwidth)
PCI	3.3 volt CPI slot compatibility only
Simultaneous Drive Transfer Channels	Two
Channel Transfer Rate	640-MB/s total; 320-MB/s per channel
Software upgradeable Firmware	Yes
Cache Memory	64 MB of DDR memory used for RAID and read cache
Logical Drives Supported	32
Maximum Capacity	2.9 TB (20 X 146.8-GB)
Memory Addressing	64-bit, supporting servers memory greater than 4-GB
RAID Support	RAID 5 (Distributed Data Guarding)
	RAID 1+0 (Striping & Mirroring)
	RAID 1 (Mirroring)
	RAID 0 (Striping)
Upgradeable Firmware	2-MB Flashable ROM
Disk Drive and Enclosure Protocol Support	Ultra 320, Ultra2 and Ultra3
Dimensions (HxWxD)	12.3 X 4.2 X 0.6 in/31.24 x 10.7 x 1.5 cm
Warranty	*Maximum:* The remaining warranty of the HP server product in which it is installed (to a maximum three-year limited warranty)
	Minimum: One-year, on-site limited warranty
	Pre-Failure Warranty: Drives attached to the Smart Array Controller and monitored under Insight Manager are supported by a Pre-Failure (replacement) Warranty. For complete details, consult the HP Support Center or refer to your HP Server Documentation.

98

SMART ARRAY 641

Protocol	Ultra320 SCSI
SCSI Electrical Interface	Low Voltage Differential (LVD)
Drives Supported	Up to 6 Ultra 320, Ultra3 and Ultra2 SCSI hard drives
SCSI Port Connectors SA-641	one internal SCSI port
Data Transfer Method	64-Bit PCI bus-master
PCI Bus Speed	64-bit, 133-MHz PCI-X (1 GB/s maximum bandwidth)
PCI	3.3 volt CPI slot compatibility only
Simultaneous Drive Transfer Channels	Two
Channel Transfer Rate	320-MB/s total; 320-MB/s per channel
Software upgradeable Firmware	Yes
Cache Memory	64 MB of DDR memory used for RAID and read cache
Logical Drives Supported	32
Maximum Capacity	880.8 GB (6 X 146.8 GB)
Memory Addressing	64-bit, supporting servers memory greater than 4 GB
RAID Support	RAID 5 (Distributed Data Guarding)
	RAID 1+0 (Striping & Mirroring)
	RAID 1 (Mirroring)
	RAID 0 (Striping)
Upgradeable Firmware	2-MB Flashable ROM
Disk Drive and Enclosure Protocol Support	Ultra 320, Ultra2 and Ultra3
Dimensions (HxWxD)	12.3 X 4.2 X 0.6 in/31.24 x 10.7 x 1.5 cm
Warranty	*Maximum:* The remaining warranty of the HP server product in which it is installed (to a maximum three-year limited warranty)
	Minimum: One-year, on-site limited warranty
	Pre-Failure Warranty: Drives attached to the Smart Array Controller and monitored under Insight Manager are supported by a Pre-Failure (replacement) Warranty. For complete details, consult the HP Support Center or refer to your HP Server Documentation.

5796

Technical Specifications

64-MB BBWC ENABLER

Cache Memory	64 MB of DDR memory for RAID, read cache, and BBWC: ECC protection, battery-backed, and removable
Cache Batteries	Up to 3 days of battery life, removable for easy replacement
Dimensions (HxWxD)	3.5 X 1.8 X .54 in/8.89 x 4.6 x 1.37 cm

Microsoft and Windows NT are US registered trademarks of Microsoft Corporation. UNIX is a registered trademark of The Open Group.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Apêndice DX

UNITED

» hp home | » products & services | » support & drivers | » solutions | » how to b

» contact hp

search:

● HP-UX operating system ○ all

HP-UX | manageability | partitions

printable ve

HP-UX virtual partitions (vPars)[1]

invent

» hp-ux home

» hp software index home
» operating and embedded home
» software strategy

» hp-ux press room

» technical support
» buy online from hp
» section map

HP-UX Virtual Partitions (vPars) enables you to run multiple instances (versions) of the HP-UX 11i Operating Environment (OE) simultaneously on one server with each OE instance hosting its own set of applications in a fully isolated environment. Created through software, virtual partitions provide application and operating systems isolation that run on single server nodes or within single-system hard partitions. Each virtual partition runs its own image of the operating system and can fully host its own applications—offering complete software isolation. The capability of CPU migration allows users to add and delete dynamically (without reboot) CPUs from one virtual partition to another. This enables applications to coexist in the same server while assuring complete privacy. In addition, functionality is provided to dynamically create, modify or even delete the isolated operating environments on a running server without interrupting non-related partitions.

In comparison to nPartitions, vPars provide greater flexibility and granularity while nPartitions provide greater fault isolation. Greater flexibility in vPars is achieved with the ability—using simple software commands—to add and delete dynamically (without reboot) CPUs from one virtual partition to another. In addition, multiple vPars can function within an nPartition providing greater granularity (1 CPU).

HP-UX Virtual Partitions (vPars) is available on the following HP servers running HP-UX Superdome, rp8400, rp7410, rp7405, rp7400, rp5470, rp5405.

partitioning inforn

» partitioning contin
» nPartitions
» virtual partitions
» information library

related informatio

» hyperplex
» workload manage
» process resource
» processor sets

benefits

vPars provides the following benefits:

- **Increased system** utilization by partitioning previously unused portions of the ser Typically, a server is only using 50% of its capacity.
- **Greater flexibility** of resources through: 1) multiple but independent operating environments per server (with as low as 1 CPU granularity per partition) and 2) th movement of CPU power between vPars depending on workload requirements.
- **Increased isolation** of applications, their operating systems, and assigned resou memory, and I/O), with individual reconfiguration and rebooting of the individual p without affecting other partitions and their applications.
- **Server consolidation** by running multiple workloads with their unique Operating configuration needs on the same server at the same time. They are excellent for c creating test platforms without investing in more hardware.

[1]At this time, vPars is available only on HP-UX 11i on certain PA-RISC servers.

privacy statement using this site means you accept its terms feedback to webmaste

Apêndice DZ

5793
21

HP System Partitions Guide

Administration for nPartitions

Sixth Edition

Revision 6.0

Manufacturing Part Number: 5187-3603
April 2003

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Copyright Notice

5791

Preface

The *HP System Partitions Guide* describes nPartition system administration procedures, concepts, and principles for HP rp7405/rp7410 servers, HP rp8400 servers, and HP Superdome servers running the HP-UX 11i operating system.

This preface has the following sections:

- *About This Book: Overview of Chapters* on page 4
- *How to Buy This Book* on page 6
- *Related Information* on page 7
- *Publication History* on page 10
- *Notational Conventions* on page 11

Reader Comments and Feedback

Hewlett-Packard welcomes your feedback on this publication. Please address your comments to `edit@presskit.rsn.hp.com` and note that you will not receive an immediate reply. All comments are appreciated.

5x90

About This Book: Overview of Chapters

1. *nPartition System Overviews* on page 31

   This chapter introduces Hewlett-Packard's nPartition system features, server models, nPartition concepts, administration tools, and HP-UX 11i support for nPartitions.

2. *Planning nPartition Configurations* on page 109

   This chapter describes how you can plan nPartition configurations for HP rp7405/rp7410, rp8400, and Superdome servers. Details include the configuration requirements for nPartitions and HP recommendations.

3. *Using Console and Service Processor Interfaces* on page 125

   This chapter covers the service processors and nPartition console interfaces available for HP's nPartition servers.

4. *An Overview of nPartition Boot and Reset* on page 161

   This chapter presents an overview of booting and reset concepts and issues for HP nPartition servers.

5. *Booting and Resetting nPartitions* on page 197

   This chapter presents procedures for booting and resetting nPartitions and procedures for configuring an nPartition's boot-related options.

6. *Managing nPartitions* on page 243

   This chapter presents the procedures for creating, configuring, and managing nPartitions on HP servers that support them.

7. *Listing and Managing Server Hardware* on page 305

   This chapter covers the tools and methods for listing details about the hardware assigned to nPartitions. This chapter also covers getting information about server hardware, and managing the hardware resources in nPartitions and their server complexes.

8. *Online Add and Replacement (OLAR) of PCI Cards* on page 365

   This chapter presents background information and procedures for performing PCI I/O card *online addition and replacement* (OLAR) on HP's nPartition servers.

5789

9. *Processor Instant Capacity on Demand (iCOD)* on page 397

   This chapter covers using Hewlett-Packard's processor iCOD (Instant Capacity on Demand) product on nPartitions.

   iCOD is an *optional* software product that enables you to instantly increase or adjust processing power within nPartitions. As you need more or fewer processors, you use iCOD tools to adjust the number of activated processors in the nPartition.

10. *Processor Sets (Psets) on nPartitions* on page 419

    This chapter describes how to use and manage processor sets (Psets) on nPartition systems.

    Using Psets, you can create multiple independent processor groups in an nPartition. Each Pset has its own processors, schedules, and attributes. Because Psets are dynamic, you can create, modify, and destroy Psets instantly as your system needs demand.

11. *Virtual Partitions (vPars) Management on nPartitions* on page 441

    This chapter describes how to create, configure, and manage HP's virtual partitions within an HP Superdome nPartition (hard partition) system environment. Each virtual partition can boot a single instance of the HP-UX B.11.11 operating system.

    The HP virtual partitions (vPars) software is an *optional* feature that you can use to further subdivide a server's resources into multiple, smaller virtual machines through software partitioning.

    By configuring multiple virtual partitions within an nPartition, you can boot multiple instances of HP-UX B.11.11 in a single nPartition.

5288

How to Buy This Book

You can purchase a printed copy of the *HP System Partitions Guide* from Hewlett-Packard's `http://software.hp.com` Web site. When at this Web site, click the **Documentation** link for a list of current publications.

The `http://www.software.hp.com/BOOKS_products_list.html` Web site lists technical books currently available for sale, including this book.

You also can find this book by searching for "Partitions Guide" using the HP software depot search facility.

5287

Related Information

For the most current HP-UX 11i nPartition administration details refer to this publication, the *HP System Partitions Guide*.

You also can find other information on general HP-UX 11i administration, HP nPartition server hardware management, and diagnostic support tools in the following publications.

Web Site for HP Technical Documentation: http://docs.hp.com

The main Web site for Hewlett-Packard technical documentation is the `http://docs.hp.com` site, which has complete information available for free.

HP-UX 11i Information

The following Web site and publications are available for info about the HP-UX 11i operating system.

- `http://docs.hp.com/hpux/os/11i/` — This is the portion of the docs.hp.com Web site that has complete HP-UX 11i information.
- *Configuring HP-UX for Peripherals*
- *HP-UX 11i June 2003 Release Notes*
- *HP-UX 11i Installation and Update Guide*
- *HP-UX Workload Manager User's Guide*
- *HP Process Resource Manager User's Guide*
- *Installing and Managing HP-UX Virtual Partitions (vPars)*
- *Instant Capacity on Demand (iCOD) and Pay Per Use (PPU) User's Guide for Version B.04.x*
- *Instant Capacity on Demand (iCOD) User's Guide for Version B.05.00*
- *Managing Systems and Workgroups: A Guide for HP-UX System Administrators*

Server Hardware Information

The following Web sites and publications describe HP nPartition server hardware management, including site prep, installation, and other details.

- `http://docs.hp.com/hpux/hw/` — This is the systems hardware portion of the docs.hp.com Web site. The following Superdome, rp8400, and rp7405/rp7410 server Web sites are available from this systems hardware page.
- **HP Superdome** — `http://docs.hp.com/hpux/hw/index.html#Superdome%20Server`

  This is the Web site for hardware info about the HP Superdome server.
- **HP rp8400** — `http://docs.hp.com/hpux/hw/index.html#rp8400%20Server`

  This is the Web site for hardware info about the HP rp8400 server.
- **HP rp7405/rp7410** — `http://docs.hp.com/hpux/hw/index.html#rp7405/rp7410%20Server`

  This is the Web site for hardware info about the HP rp7405/7410 server.

Diagnostics and Event Monitoring: Hardware Support Tools

Complete information about HP's hardware support tools, including online and offline diagnostics and event monitoring tools, is at the `http://docs.hp.com/hpux/diag/` Web site. This site has manuals, tutorials, FAQs, and other reference material.

Web Site for HP Technical Support: http://us-support2.external.hp.com

Hewlett-Packard's IT resource center Web site at `http://us-support2.external.hp.com/` provides comprehensive support information for IT professionals on a wide variety of topics, including software, hardware, and networking.

5785

Books about HP-UX Published by Prentice Hall

The `http://www.hp.com/hpbooks/` Web site lists the HP books that Prentice Hall currently publishes, such as HP-UX books including:

- *HP-UX 11i System Administration Handbook*
  `http://www.hp.com/hpbooks/prentice/ptr_0130600814.html`
- *HP-UX Virtual Partitions*
  `http://www.hp.com/hpbooks/prentice/ptr_0130352128.html`

HP Books are available worldwide through bookstores, online booksellers, and office and computer stores.

Publication History

The publication history for the *HP System Partitions Guide* includes the following editions.

Sixth Edition — April 2003, 5187-3603. CD-ROM, Web (`http://docs.hp.com/`), and print delivery.

You can order this book in print from the `http://software.hp.com` Web site.

Updates include HP rp7405 server details, vPars A.02.02 information, and other changes throughout.

Fifth Edition — August 2002, B2355-90762. CD-ROM, EPSS, Web (`http://docs.hp.com/`), and print delivery.

Fourth Edition — June 2002, B2355-90752. CD-ROM, EPSS, and Web (`http://docs.hp.com/`) delivery.

Third Edition — March 2002, B2355-90746. CD-ROM, EPSS, and Web (`http://docs.hp.com/`) delivery.

Second Edition — December 2001, B2355-90744. CD-ROM, EPSS, and Web (`http://docs.hp.com/`) delivery.

First Edition — September 2001, B2355-90736. CD-ROM, EPSS, and Web (`http://docs.hp.com/`) delivery.

5783

Notational Conventions

The following notational conventions are used in this publication.

WARNING

A warning lists requirements that you must meet to avoid personal injury.

CAUTION

A caution provides information required to avoid losing data or avoid losing system functionality.

NOTE

A note highlights useful information such as restrictions, recommendations, or important details about HP product features.

- `Commands and options` are represented using `this font`.
- **`Text that you type exactly as shown`** is represented using **`this font`**.
- *`Text to be replaced with text that you supply`* is represented using *`this font`*.

  Example:
  "Enter the `ls -l` *`filename`* command" means you must replace *`filename`* with your own text.
- **Keyboard keys and graphical interface items (such as buttons, tabs, and menu items)** are represented using **this font**.

  Examples:
  The **Control** key, the **OK** button, the **General** tab, the **Options** menu.
- **Menu —> Submenu** represents a menu selection you can perform.

  Example:
  "Select the **Partition —> Create Partition** action" means you must select the **Create Partition** menu item from the **Partition** menu.
- `Example screen output` is represented using `this font`.

5781

Contents

5779
21

S377
2l

5775
21

5774
21

Figures

5773

Tables

5772
28

Procedures

Procedures for Managing nPartitions

3770

Procedures for Listing and Managing Server Hardware

Procedures for Online Add and Replacement (OLAR) of PCI Cards

Procedures for Processor Instant Capacity on Demand (iCOD)

Procedures for Processor Sets (Psets) on nPartitions

5768

Procedures for Virtual Partitions (vPars) Management on nPartitions

5766

1 nPartition System Overviews

This chapter introduces Hewlett-Packard's nPartition system features, server models, nPartition concepts, administration tools, and HP-UX 11i support for nPartitions.

- The first sections of this chapter introduce the nPartition system environment and the HP servers that support nPartitions.
- Details about nPartition concepts are given starting with the section *Overview of nPartitions* on page 60.
- Descriptions of tools and HP-UX features for using nPartitions are given starting with the section *Tools for Managing nPartitions* on page 70.

For nPartition configuration requirements and related HP recommendations, refer to the chapter *Planning nPartition Configurations* on page 109.

For procedures to manage nPartitions, refer to the chapter *Managing nPartitions* on page 243.

Introduction

Hewlett-Packard's nPartition system capabilities enable you to configure a single server complex as one large system or as multiple smaller systems.

Each nPartition definition establishes a subset of the server hardware resources that are used as an independent system environment. An nPartition includes: one or more *cells* (containing processors and memory) that are assigned to the nPartition as well as all *I/O chassis* connected to those cells.

All processors, memory, and I/O in an nPartition are used exclusively by software running in the nPartition. Thus, each nPartition runs its own instance of the Boot Console Handler (BCH) interface and independently boots and reboots instances of HP-UX 11i.

By defining multiple nPartitions within an nPartition server, you establish hardware partitioning that enables a single server complex to run multiple instances of the HP-UX 11i operating system.

You also can establish *virtual partitions* within an nPartition on HP Superdome servers. The HP virtual partitions software enables you to further subdivide an nPartition's active hardware resources by using software partitioning to create one or more virtual partitions (vPars). Each virtual partition can load/boot HP-UX B.11.11 independently. Refer to the chapter *Virtual Partitions (vPars) Management on nPartitions* on page 441 for details.

The HP-UX 11i June 2003 release supports nPartitions on the following servers:

- HP rp7405/rp7410 server (`model` string: 9000/800/rp7410)
- HP rp8400 server (`model` string: 9000/800/S16K-A)
- HP Superdome 16-way (`model` string: 9000/800/SD16000)
- HP Superdome 32-way (`model` string: 9000/800/SD32000)
- HP Superdome 64-way (`model` string: 9000/800/SD64000)

For server hardware details see *Supported HP Server Models* on page 34.

S764

You can reconfigure a server's nPartition definitions without physically modifying the server's hardware configuration by using HP's software-based nPartition management tools.

You can reconfigure any nPartition to include more, fewer, and/or different hardware resources. Doing this requires shutting down the operating system running in the nPartition and resetting the nPartition to reconfigure it; this *reboot for reconfig* operation is performed using the `shutdown -R` HP-UX command (using the `-R` option, not `-r`).

With HP's nPartition servers, you can start with a system that meets your needs now and add more components (cells and I/O) as your needs increase.

For example, with a Superdome server you can add cells, I/O chassis, and/or upgrade to larger-capacity systems as needed. A Superdome 16-way server can be upgraded to a Superdome 32-way server, and likewise the Superdome 32-way server can be upgraded to Superdome 64-way server. You also can add I/O expansion cabinets to a Superdome server at any time.

Administration Tools for nPartitions

You can use several administration tools to manage nPartitions in a server complex, including the service processor, consoles, Boot Console Handler (BCH) interfaces, HP-UX commands, and Partition Manager.

- Server complex's **service processor (GSP or MP)**, which includes the Command menu, partition consoles, partition Virtual Front Panels, partition Console Logs, and the Chassis Log viewer.
- **nPartition console and BCH interface**, which provides console access (through the service processor) as well as interactive control before HP-UX has booted on an nPartition.
- **HP-UX nPartition commands** (including `parstatus`, `parcreate`, `parmodify`, and others) enable you to list, monitor, configure, and manage nPartitions from HP-UX.
- The **Partition Manager** utility (`/opt/parmgr/bin/parmgr`) provides a graphical interface for listing and managing nPartitions.

See *Tools for Managing nPartitions* on page 70 for more details.

5763

Supported HP Server Models

The HP servers that support nPartitions include the following models:

- HP rp7405/rp7410 server—See *rp7405 / rp7410 Server Model* on page 36.
- HP rp8400 server—See *rp8400 Server Model* on page 38.
- Three models of HP Superdome servers—See *Superdome Server Models* on page 40.

These nPartition servers have different hardware configurations and limits, as described in the following sections, and all include support for nPartitions.

Within each HP nPartition **server cabinet** are multiple **cells**, each of which contains processors and memory. The nPartition cabinets are shown in Figure 1-1 on page 35; cells are discussed in *Cells* on page 47.

Each nPartition server cabinet also may have multiple **I/O chassis** that provide PCI slots for I/O cards. Each I/O chassis connects to one of the cells in the server. See *nPartition I / O Chassis and PCI Card Slots* on page 48.

HP Superdome servers also support optional **I/O expansion cabinets** to provide additional I/O chassis. See *I / O Chassis in HP Superdome IOX Cabinets* on page 51.

All hardware within a server—including all cells, I/O chassis, cables, cabinet hardware, and power and utilities components—is considered to be a **server complex**.

An HP Superdome complex can consist of one cabinet or two server cabinets, and can also include one or two I/O expansion cabinets (to provide additional I/O chassis).

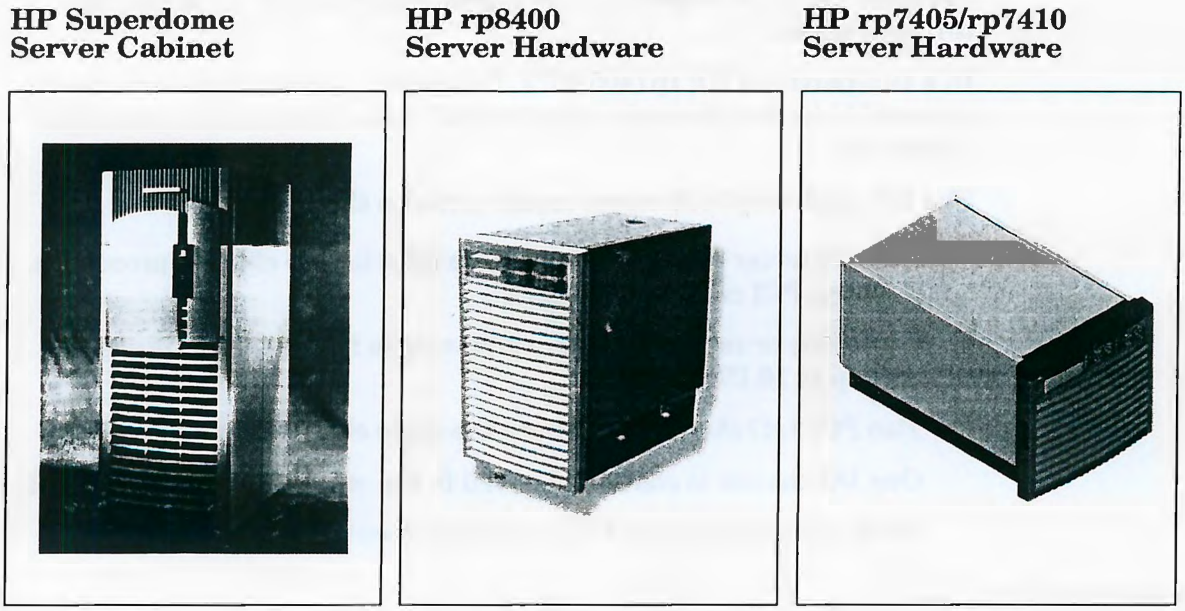
Each HP rp7405/rp7410 or HP rp8400 server complex consists of a single server cabinet only.

5762
21

Hardware Models: Superdome, rp8400, and rp7405/rp7410 nPartition Servers

HP Superdome, HP rp8400, and HP rp7405/rp7410 server cabinets are shown in Figure 1-1.

Figure 1-1 **HP nPartition Server Hardware**



HP Superdome Server Cabinet

HP rp8400 Server Hardware

HP rp7405/rp7410 Server Hardware

rp7405/rp7410 Server Model

HP rp7405/rp7410 servers scale from one to two cells and include complete support for hard partitions (nPartitions).

Figure 1-2 on page 37 shows an overview of the HP rp7405/rp7410 server hardware architecture.

You can configure a single nPartition using one or both cells, or can configure up to two separate nPartitions within an HP rp7405/rp7410 server complex.

In a two-partition HP rp7405/rp7410 complex, you would use cell 0 and its core I/O in one nPartition, and use cell 1 and its core I/O in the other nPartition.

The HP rp7405/rp7410 server model includes these features:

- *A single server cabinet* that includes all cells, I/O chassis, processors, memory, PCI cards, and core I/O.
- *Either one or two cells.* Each cell has up to four PA-RISC processors and up to 16 DIMMs.
- *Two PCI I/O chassis* that share the same chassis hardware.

  One I/O chassis is connected to cell 0, the other is connected to cell 1.

  Each I/O chassis has 8 PCI card slots, numbered from 1 to 8.

NOTE On HP rp7405/rp7410 servers, two PCI slots by convention are dedicated for use by a combination LAN/SCSI card: PCI domain 0 slot 1 (the first slot on the left) and PCI domain 1 slot 8 (the last slot on the right).

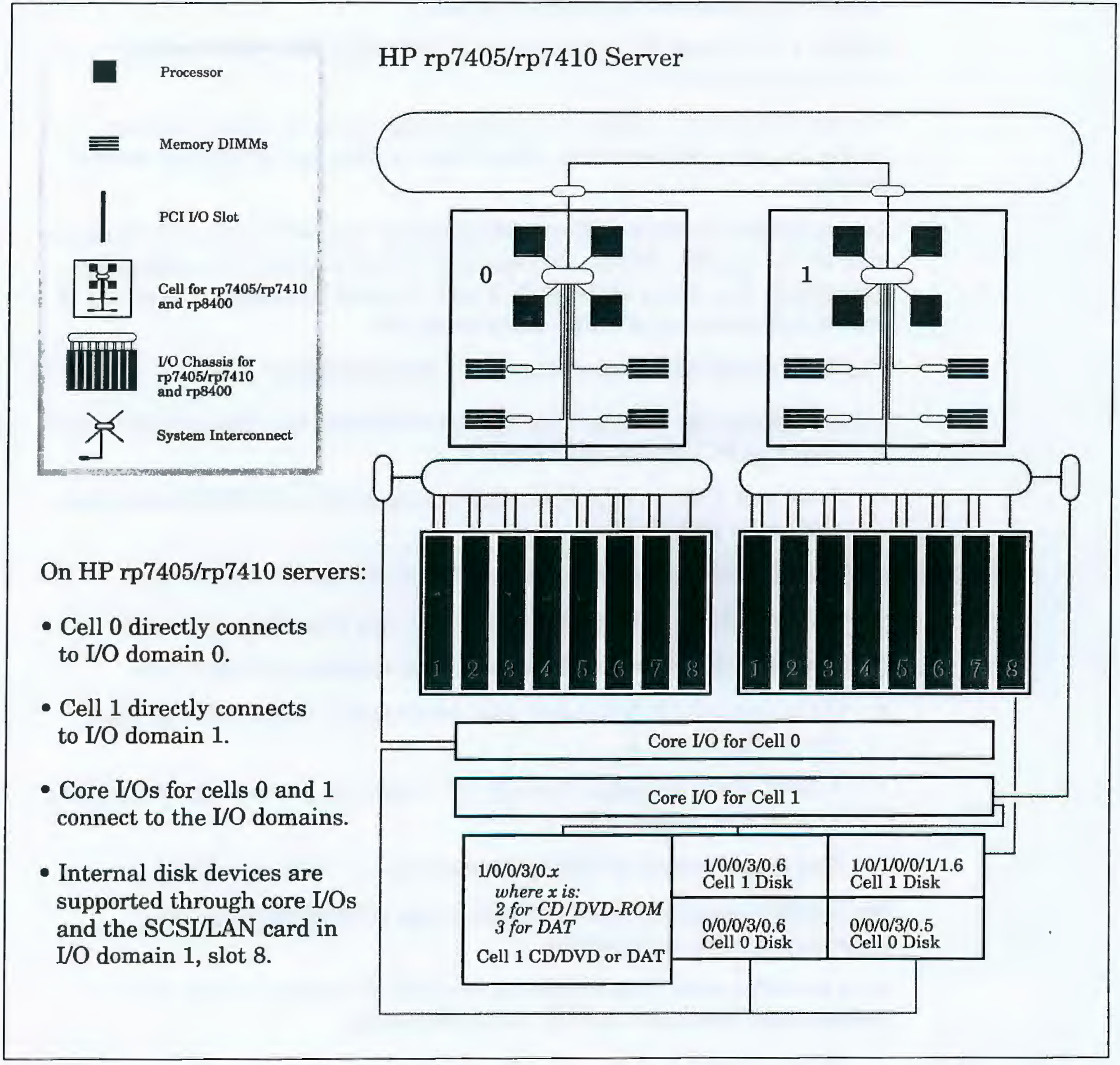
- *Up to two core I/O devices*, one connected to cell 0, and the other connected to cell 1.
- *A total server complex capacity of*: 2 cells, 8 processors, 32 DIMMs, and 16 PCI card slots.
- The model string for HP rp7405/rp7410 servers is `9000/800/rp7410`.

HP rp7405/rp7410 servers currently include a single server cabinet that is rack-mounted only. In the future HP also will support a stand-alone HP rp7405/rp7410 server configuration.

S760
2D

Also see *nPartition System Hardware Details* on page 47 for more information about HP rp7405/rp7410 server features.

Figure 1-2 **HP rp7405/rp7410 Server Architecture Overview**



On HP rp7405/rp7410 servers:

- Cell 0 directly connects to I/O domain 0.
- Cell 1 directly connects to I/O domain 1.
- Core I/Os for cells 0 and 1 connect to the I/O domains.
- Internal disk devices are supported through core I/Os and the SCSI/LAN card in I/O domain 1, slot 8.

5759

rp8400 Server Model

HP rp8400 servers scale from one to four cells and include complete support for hard partitions (nPartitions).

Figure 1-3 on page 39 shows an overview of the HP rp8400 server hardware architecture.

You can configure a single nPartition using some or all cells, or can configure up to two separate nPartitions within an HP rp8400 server complex.

In a multiple-partition HP rp8400 complex, you would use cell 0 and its core I/O in one nPartition, and use cell 1 and its core I/O in the other nPartition. Any other cells (cells 2 and 3) could be assigned to either of the two nPartitions, or could be unassigned.

The HP rp8400 server model includes these features:

- *A single server cabinet* that includes all cells, I/O chassis, processors, memory, PCI cards, and core I/O.
- *From one to four cells*. Each cell has up to four PA-RISC processors and up to 16 DIMMs.
- *Two PCI I/O chassis* that share the same chassis hardware.

  One I/O chassis is connected to cell 0, the other is connected to cell 1.

  Each I/O chassis has 8 PCI card slots, numbered from 1 to 8.
- *Up to two core I/O devices*, one connected to cell 0, and the other connected to cell 1.
- *A total server complex capacity of*: 4 cells, 16 processors, 64 DIMMs, and 16 PCI card slots.
- The model string for HP rp8400 servers is `9000/800/S16K-A`.

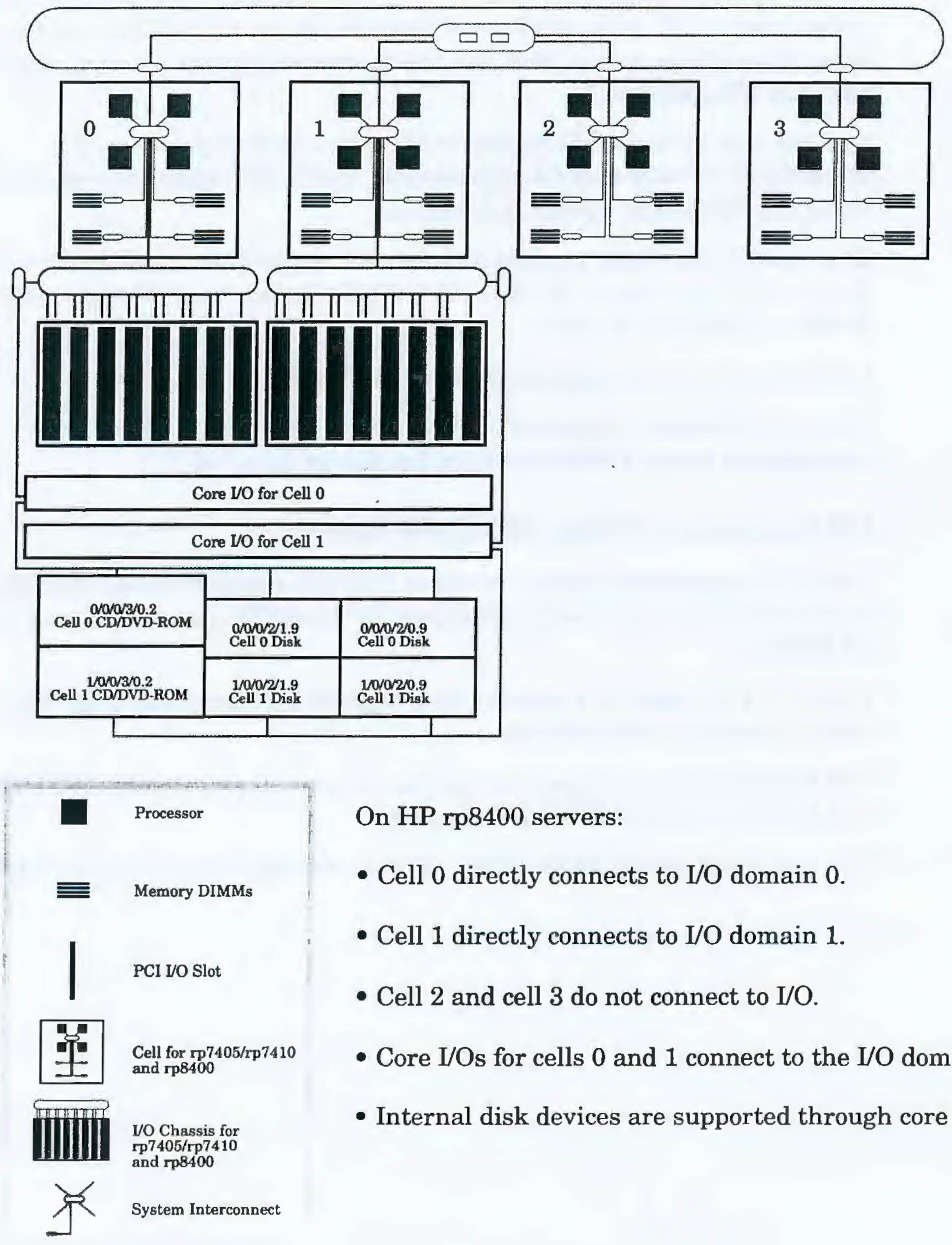
HP rp8400 servers include a single server cabinet that can be rack-mounted or stand-alone.

Also see *nPartition System Hardware Details* on page 47 for more information about HP rp8400 server features.

5758

Figure 1-3 HP rp8400 Server Architecture Overview

HP rp8400 Server



On HP rp8400 servers:

- Cell 0 directly connects to I/O domain 0.
- Cell 1 directly connects to I/O domain 1.
- Cell 2 and cell 3 do not connect to I/O.
- Core I/Os for cells 0 and 1 connect to the I/O domains.
- Internal disk devices are supported through core I/Os.

5757

Superdome Server Models

HP Superdome servers scale up to 16 cells and include complete support for hard partitions (nPartitions). You can configure a single nPartition using some or all cells, or can configure multiple nPartitions within the same Superdome server complex (up to one nPartition for each cell that has core I/O attached).

You can add up to two Superdome I/O expansion cabinets to the Superdome 32-way and 64-way models. Each I/O expansion cabinet has up to six additional 12-slot I/O chassis.

The three Superdome models include: *HP Superdome 16-Way (SD16000) Server*, *HP Superdome 32-Way (SD32000) Server*, and *HP Superdome 64-Way (SD64000) Server*.

Details on these models are given in the following sections.

Also see *nPartition System Hardware Details* on page 47 for more information about HP Superdome hardware features.

HP Superdome 16-Way (SD16000) Server

The HP Superdome 16-way server is a single-cabinet server that has from two to four cells, each with four HP PA-RISC processors and up to 32 DIMMs.

Figure 1-4 on page 41 shows an overview of the Superdome 16-way server hardware architecture.

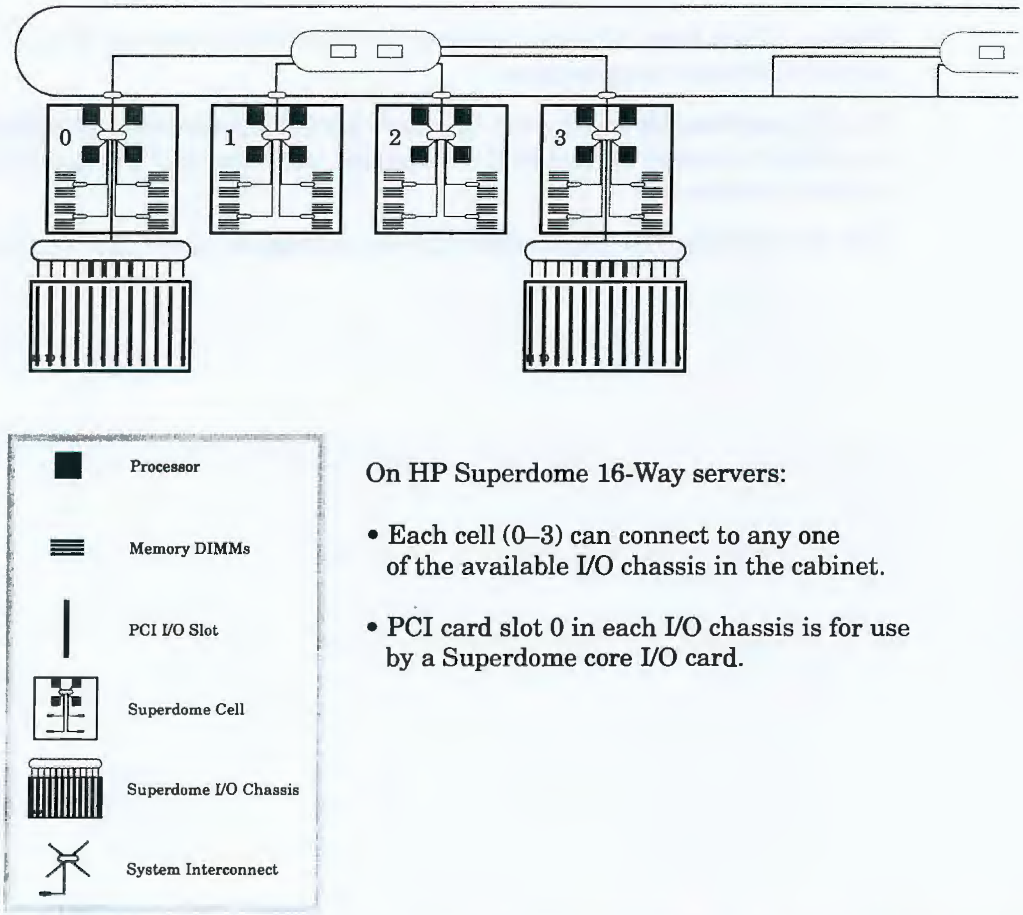
The Superdome 16-way server can have up to 16 processors, 128 DIMMs, and up to four 12-slot PCI I/O chassis.

The model string for Superdome 16-way servers is `9000/800/SD16000`.

5756

Figure 1-4 HP Superdome 16-Way Architecture Overview

HP Superdome 16-Way Server (SD16000)



On HP Superdome 16-Way servers:

- Each cell (0–3) can connect to any one of the available I/O chassis in the cabinet.
- PCI card slot 0 in each I/O chassis is for use by a Superdome core I/O card.

5755

HP Superdome 32-Way (SD32000) Server

The Superdome 32-way server is a single-cabinet server that has from two to eight cells, each with four HP PA-RISC processors and up to 32 DIMMs.

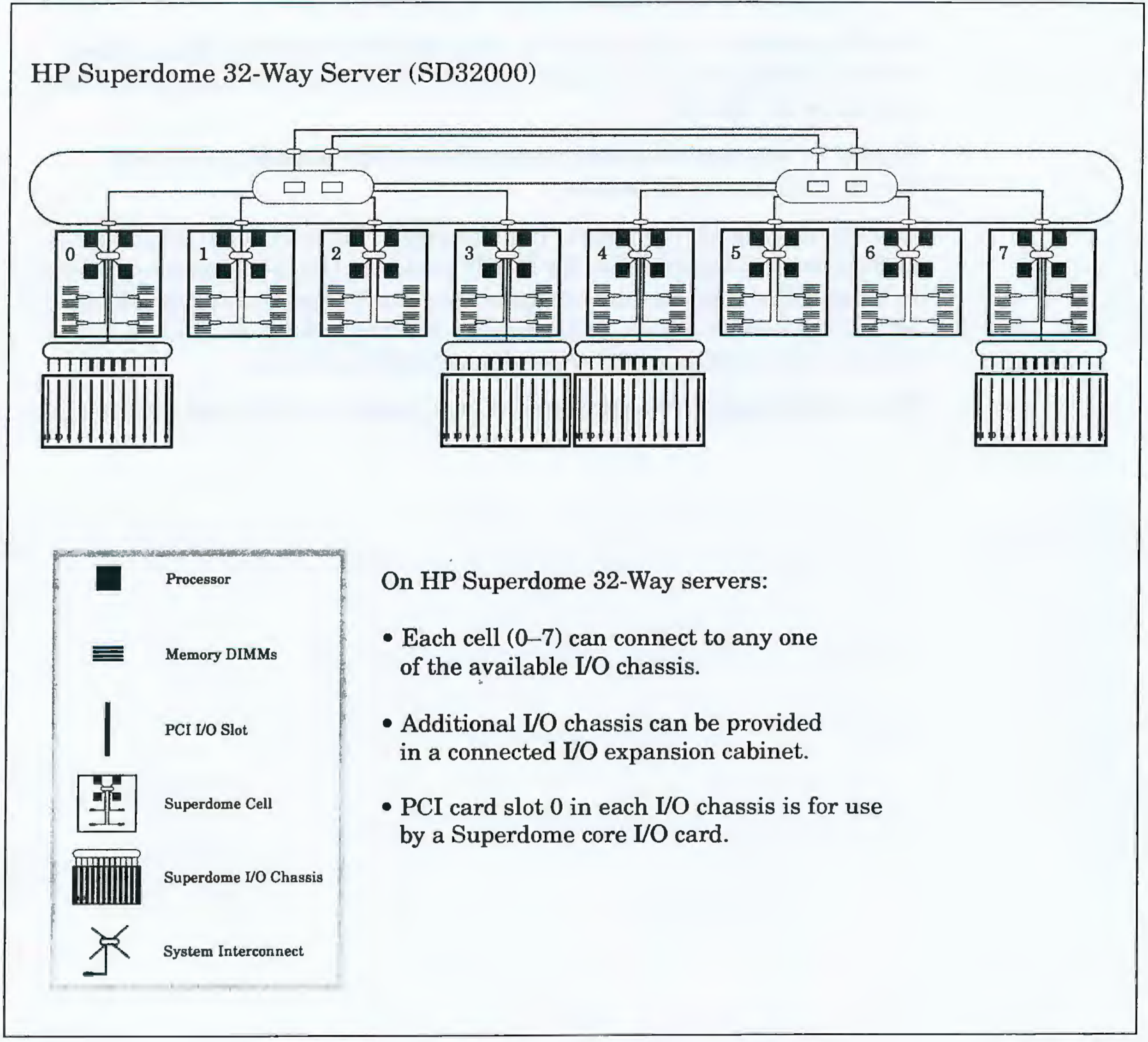
Figure 1-5 on page 43 shows an overview of the Superdome 32-way server hardware architecture.

The Superdome 32-way server can have up to 32 processors, 256 DIMMs, up to four internal 12-slot PCI I/O chassis, plus optional I/O expansion cabinet hardware.

The model string for Superdome 32-way servers is `9000/800/SD32000`.

57 54
21

Figure 1-5 **HP Superdome 32-Way Architecture Overview**



On HP Superdome 32-Way servers:

- Each cell (0–7) can connect to any one of the available I/O chassis.
- Additional I/O chassis can be provided in a connected I/O expansion cabinet.
- PCI card slot 0 in each I/O chassis is for use by a Superdome core I/O card.

HP Superdome 64-Way (SD64000) Server

The Superdome 64-way server is a tightly interconnected dual-cabinet server that has from 4 to 16 cells, each with four HP PA-RISC processors and up to 32 DIMMs.

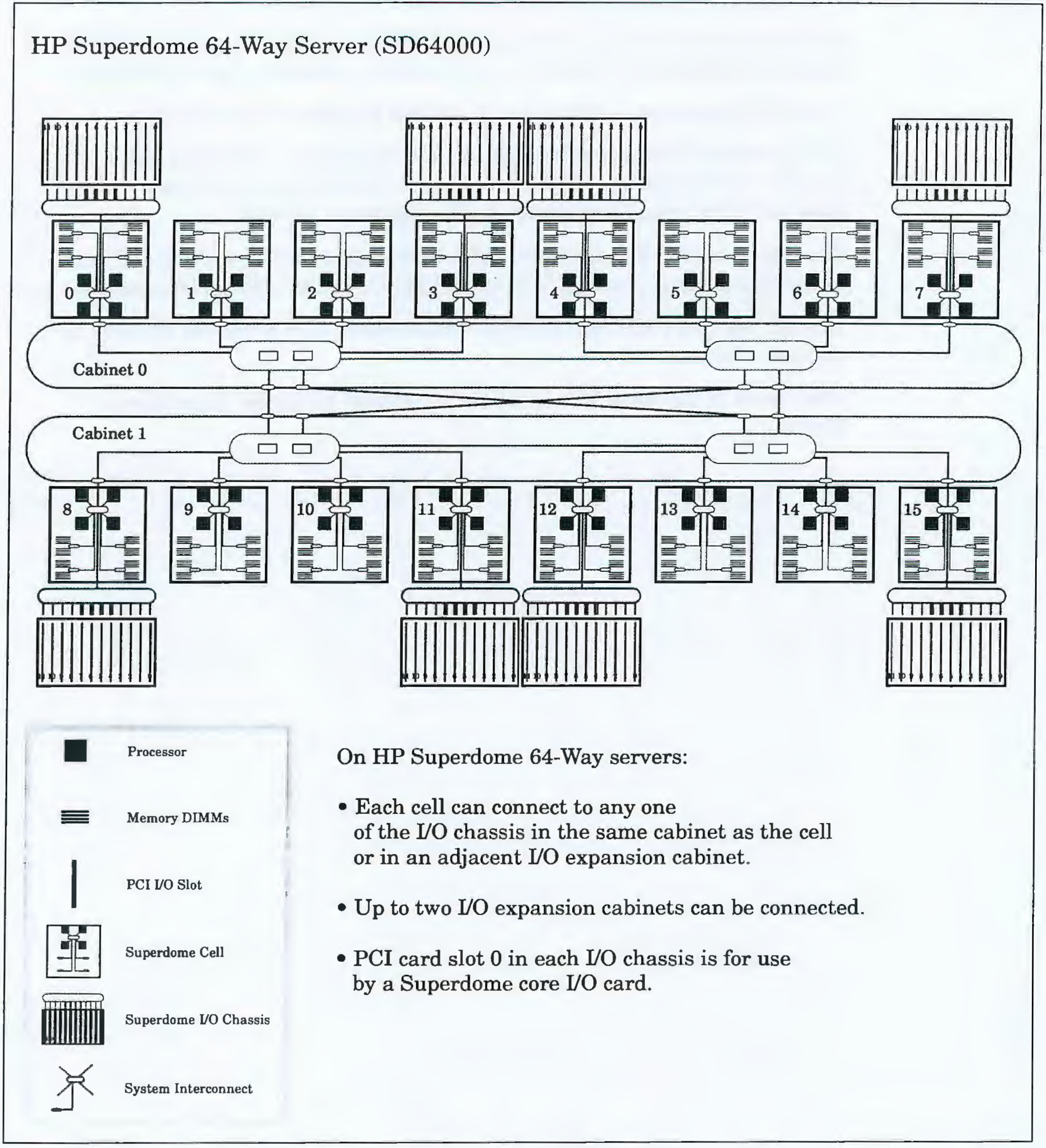
Figure 1-6 on page 45 shows an overview of the Superdome 64-way server hardware architecture.

The Superdome 64-way server can have up to 64 processors, 512 DIMMs, and up to eight internal 12-slot PCI I/O chassis. (Each of the two cabinets in a Superdome 64-way server provides up to 32 processors, 256 DIMMs, and up to four 12-slot PCI I/O chassis.) HP Superdome 64-way servers also can have optional I/O expansion cabinet hardware.

The model string for Superdome 64-way servers is `9000/800/SD64000`.

5x52

Figure 1-6 **HP Superdome 64-Way Architecture Overview**



On HP Superdome 64-Way servers:

- Each cell can connect to any one of the I/O chassis in the same cabinet as the cell or in an adjacent I/O expansion cabinet.
- Up to two I/O expansion cabinets can be connected.
- PCI card slot 0 in each I/O chassis is for use by a Superdome core I/O card.

5751

HP Superdome I/O Expansion Cabinet

HP Superdome 32-way and Superdome 64-way servers can include I/O expansion cabinets in addition to the server cabinet(s) in the complex.

Each I/O expansion cabinet has a cabinet number of either 8 or 9.

A Superdome I/O expansion cabinet includes up to 3 I/O bays, with two 12-slot I/O chassis in each bay. This provides for up to 6 chassis with a total of 72 PCI card slots in each I/O expansion cabinet.

The Superdome I/O expansion cabinet is a standard-size cabinet that, space permitting, you can mount peripherals in as well as I/O chassis.

See the section *I/O Chassis in HP Superdome IOX Cabinets* on page 51 for more details.

Also refer to the book *I/O Expansion Cabinet Guide for Superdome Servers*.

5750
21

nPartition System Hardware Details

This section gives physical details about the Hewlett-Packard servers that support nPartitions, including HP Superdome, rp8400, and rp7405/rp7410 servers.

The following nPartition server hardware topics are covered here:

- *Cells* on page 47
- *Processors: HP PA-RISC CPUs* on page 48
- *nPartition I/O Chassis and PCI Card Slots* on page 48
- *Internal Disk Devices for HP rp7405/rp7410 and rp8400 Servers* on page 55
- *nPartition Service Processor (GSP or MP) Hardware* on page 56

Also see *Supported HP Server Models* on page 34 for an introduction to the HP nPartition-capable server models, including architectural overviews.

Cells

This section briefly describes cell hardware details for HP's nPartition servers.

Each cell in an HP nPartition server contains HP PA-RISC processors, memory DIMMs, and provides the connection to any I/O chassis attached to the cell.

For details about cell ID formats, see *Specifying Cells and I/O Chassis to Commands* on page 87. For details about configurable cell attributes, see *Cell Properties* on page 61.

All cells assigned to an nPartition **must** have the same firmware revisions and the same type/speed of processors and **should** have identical memory configurations. On HP servers that have multiple nPartitions, each nPartition can have different types of cells.

All processors in a cell **must** be of the same type and speed. All memory DIMMs in a cell **should** be identical for best performance.

In *HP Superdome* servers, each cell can support up to 32 memory DIMMs and 1–4 processors.

5749

In *HP rp7405/rp7410 and rp8400* servers, each cell can support up to 16 memory DIMMs and 1–4 processors.

Each HP Superdome cell can be connected to an I/O chassis that resides either in the same cabinet as the cell or in an I/O expansion cabinet.

In HP rp7405/rp7410 and rp8400 servers, cell 0 connects to I/O chassis 0, and cell 1 connects to I/O chassis 1.

Processors: HP PA-RISC CPUs

This section describes the supported processor (CPU) types for HP nPartition servers.

Within each cell in an nPartition server, *all processors* must operate at the same speed. If multiple cells reside in a server, each cell can run a set of processor whose operating speed is different from the processors in the other cell(s) in the server.

In HP Superdome cells, the following processors types are supported: PA8600 (552 MHz) or PA8700 (650, 750, or 875 MHz).

In HP rp7405/rp7410 and rp8400 servers, the supported processor types are: PA8700 (650, 750, or 875 MHz).

To list the operating speed of processors in a cell, you can use the `parstatus` HP-UX command or the `PR` command from an nPartition's BCH Information menu.

For example, `parstatus -V -c 2` lists hardware details about cell 2, including the operating speed and processor type for the cell.

Refer to the chapter *Listing and Managing Server Hardware* on page 305 for details on listing cell processor info, including a reference chart of cell processor frequencies.

nPartition I/O Chassis and PCI Card Slots

This section has details about the I/O chassis and PCI card slot locations in various models of HP nPartition servers and I/O expansion cabinets, and details about slot frequencies and power capabilities.

The following I/O chassis and slots are discussed here:

- *I/O Chassis in HP Superdome Compute Cabinets* on page 49

5748

- *I/O Chassis in HP Superdome IOX Cabinets* on page 51
- *I/O Chassis for HP rp7405/rp7410 and rp8400 Servers* on page 54

I/O Chassis in HP Superdome Compute Cabinets

Each HP Superdome I/O chassis can connect to one cell in the same compute cabinet.

A Superdome I/O chassis has 12 slots, numbered from 11 to 0. The HP Superdome core I/O card *fits only in slot 0.*

Card slot details for Superdome I/O chassis are in Table 1-1.

Table 1-1 HP Superdome I/O Chassis: Card Slot Details

Slot Number	11	10	9	8	7	6	5	4	3	2	1	0
Signaling (Volts)	5.0 / 3.3				3.3				5.0 / 3.3			
Hardware Fabric	single rope				dual rope				single rope			
Cards Accepted	PCI cards keyed as 5-volt or universal.				PCI cards keyed as 3.3-volt or universal.				PCI cards keyed as 5-volt or universal.			

In HP Superdome I/O chassis, all slots can operate as 64-bit slots and can accept 66 MHz PCI cards.

HP Superdome I/O chassis slots 0–3 and 8–11 can accept cards that are physically keyed as 5-volt cards or are keyed as universal cards. These slots normally operate at 33 MHz with 5-volt signaling, but when a 66 MHz capable card is detected they are switched by software to operate at 66 MHz with 3.3-volt signaling.

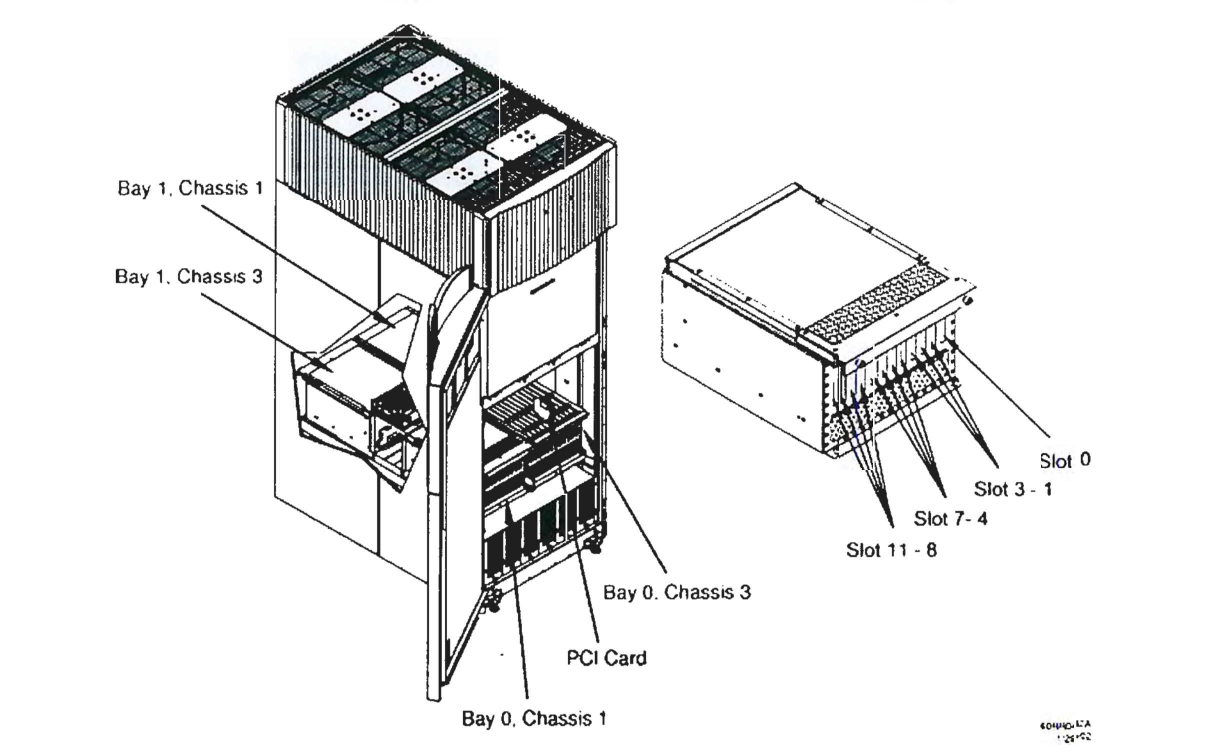
Slots 4–7 in a Superdome I/O chassis can accept cards that are physically keyed as 3.3-volt cards or are keyed as universal cards. These slots can operate at 66 MHz or 33 MHz with 3.3-volt signaling only.

Slots 4–7 also are **dual-rope slots**, which have two connections between the slot's local bus adapter (LBA) and the I/O chassis system bus adapter (SBA). All other slots are **single-rope slots**, which have a single connection between the slot LBA and the I/O chassis SBA. The dual-rope slots can have greater sustained bandwidth than single-rope slots.

5747

The Superdome I/O chassis and slot locations are shown in Figure 1-7.

Figure 1-7 **HP Superdome I/O Chassis and PCI Card Slot Locations**



As Figure 1-7 shows, I/O chassis in HP Superdome compute cabinets reside both in the cabinet's front (I/O bay 0) and its rear (I/O bay 1). When you face each I/O bay, the left I/O chassis is chassis 1 and the right chassis is I/O chassis 3. In I/O chassis in a Superdome compute cabinet, PCI slot 11 is to the left and slot 0 is to the right.

In HP Superdome I/O expansion cabinets, the I/O chassis are identical but are positioned sideways, with either slot 0 or slot 11 at the bottom.

Accessing Superdome Compute Cabinet I/O Chassis and PCI Slots

Step 1. To access the I/O chassis in an HP Superdome compute cabinet, you must open either the cabinet's front door (to access I/O bay 0) or its rear door (to access I/O bay 1). In each I/O bay—when facing the bay—I/O chassis 1 is on the left and chassis 3 is on the right.

See Figure 1-7 on page 50 for details.

Step 2. To access the PCI card slots in an HP Superdome compute cabinet's I/O chassis, you must remove the cover from the top of the I/O chassis.

In each Superdome compute cabinet I/O chassis—when facing the chassis—PCI slot 0 is on the right and PCI slot 11 is on the left.

I/O Chassis in HP Superdome IOX Cabinets

Up to two I/O expansion (**IOX**) cabinets can reside in an HP Superdome complex.

I/O expansion cabinets are numbered cabinets 8 and 9.

The IOX cabinet uses the same I/O chassis as the Superdome compute cabinet. Each IOX I/O chassis has 12 slots, numbered from 11 to 0. See Table 1-1 on page 49 for details about the card slots.

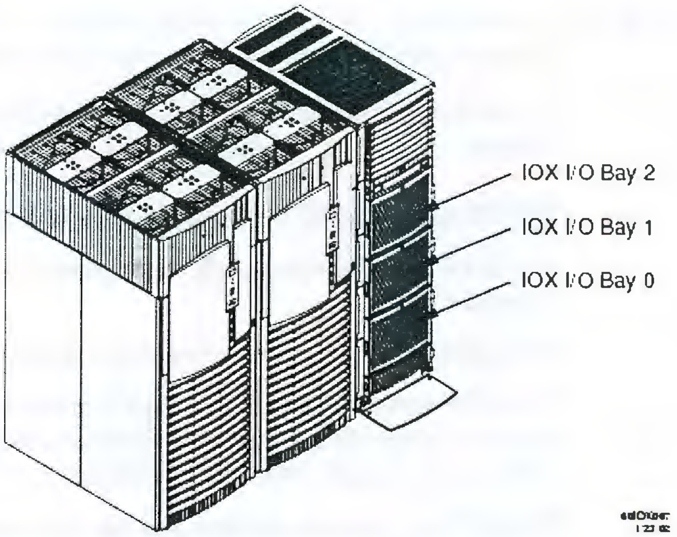
Each I/O expansion cabinet has its own power supplies, fans, and utilities (which are connected to the Superdome server's service processor bus).

The I/O chassis (and PCI card slots) within each I/O expansion cabinet are made available to nPartitions through direct I/O chassis-to-cell connections—exactly as internal Superdome server cabinet I/O chassis are connected to cells.

Three I/O bays can be housed in each IOX. These bays are numbered from bottom to top: I/O bay 0, bay 1, and bay 2, as shown in Figure 1-8.

Figure 1-8 **I/O Expansion Cabinet (IOX) for HP Superdome**

5745



Each I/O bay in an IOX houses two I/O chassis: the left chassis is I/O chassis 1, right is chassis 3. Thus, an IOX can have up to six I/O chassis that can connect to the cells in an attached Superdome compute cabinet.

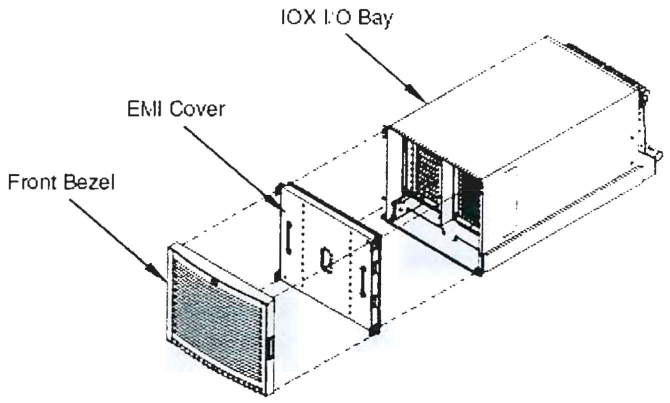
Accessing Superdome IOX I/O Chassis and PCI Card Slots

This procedure describes how to access the I/O chassis and PCI card slots in an HP Superdome I/O expansion cabinet (IOX).

Step 1. To access the I/O chassis in an IOX bay, you must remove the front bezel from the bay, and also remove the EMI cover, as shown in Figure 1-9.

The two I/O chassis in each IOX bay are accessible when the I/O bay slides out from the IOX cabinet.

Figure 1-9 IOX Bezel, Cover, and Bay



Step 2. To access the PCI card slots in an IOX I/O chassis, remove the I/O chassis cover.

To access slots in chassis 1 of the bay remove the cover from the *left* side of the I/O bay, or remove the cover from the *right* side of the bay to access I/O chassis 3's PCI card slots. See Figure 1-9 for details.

I/O Chassis for HP rp7405/rp7410 and rp8400 Servers

HP rp7405/rp7410 and rp8400 servers have two I/O chassis, each with 8 slots numbered left to right from 1 to 8.

Both HP rp7405/rp7410 and rp8400 server cabinets have a single I/O bay on the cabinet's rear that houses the two I/O chassis or "I/O domains". When you face the I/O bay, viewing the rear of the cabinet, the chassis on the left is I/O chassis 0, and right is I/O chassis 1.

Cell 0 connects to chassis 0 and cell 1 connects to chassis 1.

In HP rp7405/rp7410 servers, two PCI card slots *are reserved* for use by a SCSI/LAN card: chassis 0, slot 1 and chassis 1, slot 8. This is a 64-bit card that operates at 66 MHz and 3.3-volt signaling.

HP rp7405/rp7410 and rp8400 I/O chassis card slot details are listed in Table 1-2.

Table 1-2 **HP rp7405/rp7410 and rp8400 I/O Chassis: Card Slot Details**

Slot Number	1	2	3	4	5	6	7	8
Signaling (Volts)	3.3	3.3	3.3	3.3	3.3	3.3	5.0 / 3.3	5.0 / 3.3
Hardware Fabric	dual rope							single rope
Cards Accepted	PCI cards keyed as 3.3-volt or universal.						PCI cards keyed as 5-volt or universal.	

All slots in HP rp7405/rp7410 and rp8400 I/O chassis can operate as 64-bit slots and can accept 66 MHz PCI cards.

HP rp7405/rp7410 and rp8400 I/O chassis slots 1–6 accept cards physically keyed as 3.3-volt cards or keyed as universal cards. These slots can operate at 66 MHz or 33 MHz with 3.3-volt signaling only.

Slots 7 and 8 in rp7405/rp7410 and rp8400 I/O chassis accept cards keyed as 5-volt cards or keyed as universal cards. These slots normally operate at 33 MHz with 5-volt signaling, but when a 66 MHz capable card is detected they are switched by software to operate at 66 MHz with 3.3-volt signaling.

5742

On both HP rp7405/rp7410 and rp8400 servers, slots 1–7 are **dual-rope slots**, which have two connections between the slot's local bus adapter (LBA) and the I/O chassis system bus adapter (SBA). The core I/O connections (slot 0) and slot 8 are **single-rope slots**, which have a single connection between the slot LBA and the I/O chassis SBA. The dual-rope slots can have greater sustained bandwidth than single-rope slots.

Internal Disk Devices for HP rp7405/rp7410 and rp8400 Servers

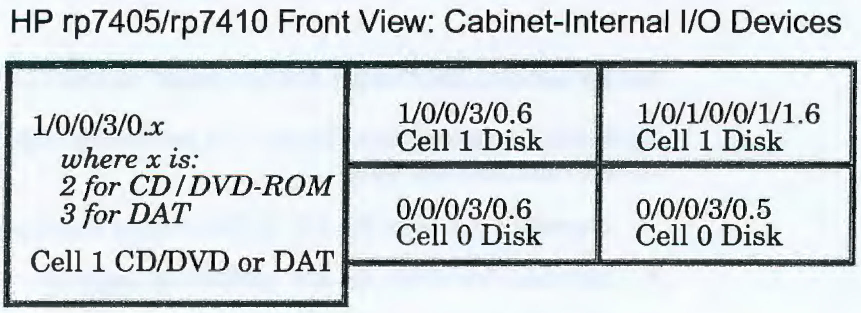
This section covers hardware paths and locations for the internal disk devices in rp7405/rp7410 and rp8400 servers:

- *Disk Devices in HP rp7405 / rp7410 Cabinets* on page 55
- *Disk Devices in HP rp8400 Cabinets* on page 56

Disk Devices in HP rp7405/rp7410 Cabinets

The hardware paths for internal drives in an HP rp7405/rp7410 cabinet are shown in Figure 1-10.

Figure 1-10 **HP rp7405/rp7410 Internal Storage Hardware Paths**



HP rp7405/rp7410 Front View: Cabinet-Internal I/O Devices

1/0/0/3/0.*x* *where x is:* *2 for CD / DVD-ROM* *3 for DAT* Cell 1 CD/DVD or DAT	1/0/0/3/0.6 Cell 1 Disk	1/0/1/0/0/1/1.6 Cell 1 Disk
	0/0/0/3/0.6 Cell 0 Disk	0/0/0/3/0.5 Cell 0 Disk

As Figure 1-10 shows, in an HP rp7405/rp7410 cabinet the top internal disk drives connect to cell 1 through the core I/O for cell 1 (for 1/0/0/3/0.6) and the LAN/SCSI card in slot 1_8 (I/O chassis 1 slot 8, for 1/0/1/0/0/1/1.6).

Both of the bottom disk drives (0/0/0/3/0.6 and 0/0/0/3/0.5) connect to cell 0 through the core I/O for cell 0.

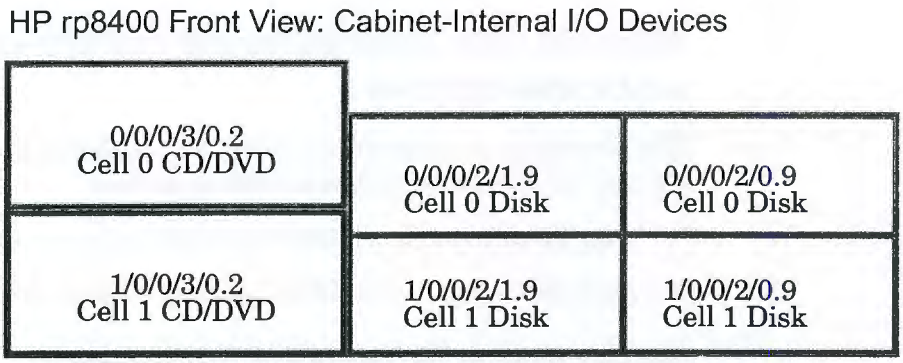
A CD/DVD-ROM drive or DAT drive connects to cell 1 through the core I/O card for cell 1, thus it can be accessed through cell 1's nPartition only.

5241

Disk Devices in HP rp8400 Cabinets

The hardware paths for internal drives in an HP rp8400 cabinet are shown in Figure 1-11.

Figure 1-11 **HP rp8400 Internal Storage Hardware Paths**



As Figure 1-11 shows, in an HP rp8400 cabinet the top internal drives connect to cell 0 through its core I/O card, and the bottom internal drives connect to cell 1 through the cell 1 core I/O card.

nPartition Service Processor (GSP or MP) Hardware

This section introduces the service processor (GSP or MP) hardware in HP's nPartition servers:

- *Service Processor for HP rp7405 / rp7410* on page 57
- *Service Processor for HP rp8400* on page 58
- *Service Processor for HP Superdome* on page 59

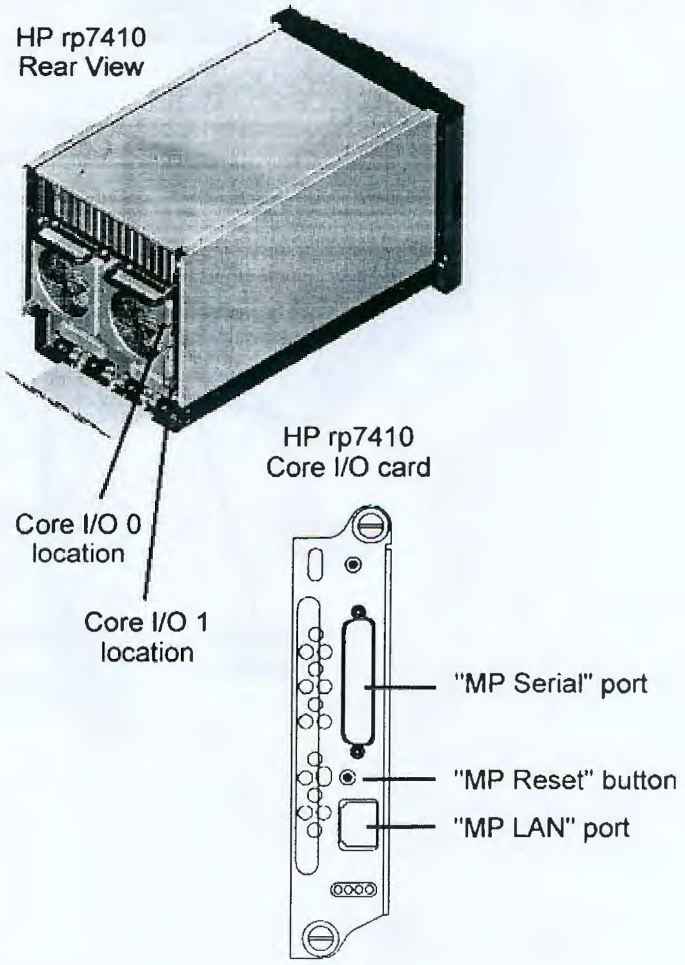
For further details on connecting to and using an nPartition server's service processor, refer to the chapter *Using Console and Service Processor Interfaces* on page 125.

S7410
21

Service Processor for HP rp7405/rp7410

On HP rp7405/rp7410 servers, service processor functionality is provided in the core I/O card, shown in Figure 1-12. The rp7405/rp7410 core I/O card's customer LAN port, which permits remote telnet access to the service processor, is labeled "MP LAN". The "MP Serial" port is single DB25 serial port from which three DB9 serial connectors are available (a DB25-to-3xDB9 dongle must be connected). A direct RS-232 serial connection to the service processor is available through the DB9 connector labeled "Console". Remote modem access to the service processor can be provided through the DB9 connector labeled "Remote".

Figure 1-12 **HP rp7405/rp7410 Service Processor LAN and Serial Ports**

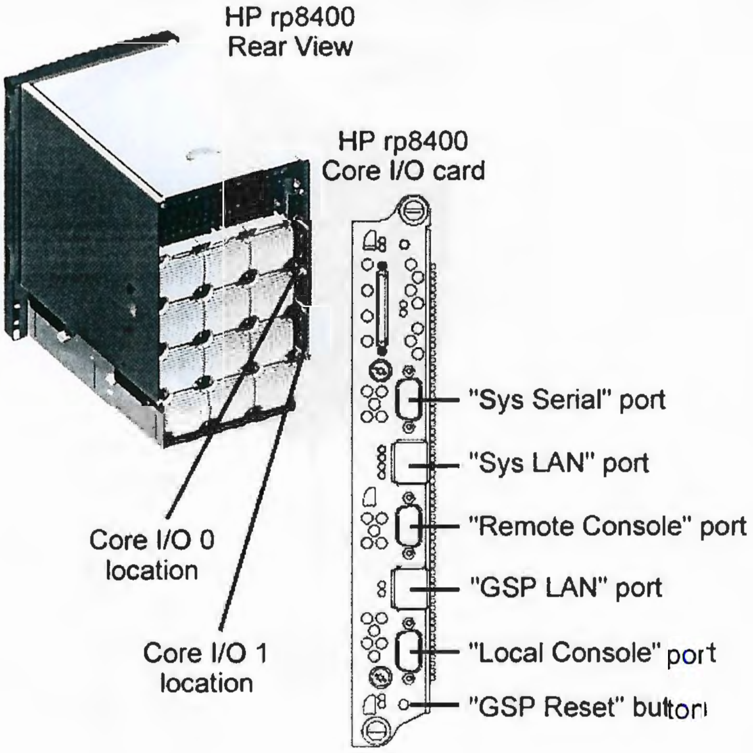


S739

Service Processor for HP rp8400

On HP rp8400 servers, service processor functionality is provided in the core I/O card, shown in Figure 1-13. The rp8400 core I/O card's customer LAN port, which permits remote telnet access to the service processor, is labeled "GSP LAN". A direct RS-232 serial connection to the service processor is available through the "Local Console" port. The "Remote Console" port is for external, remote modem access to the service processor.

Figure 1-13 **HP rp8400 Service Processor LAN and Serial Ports**

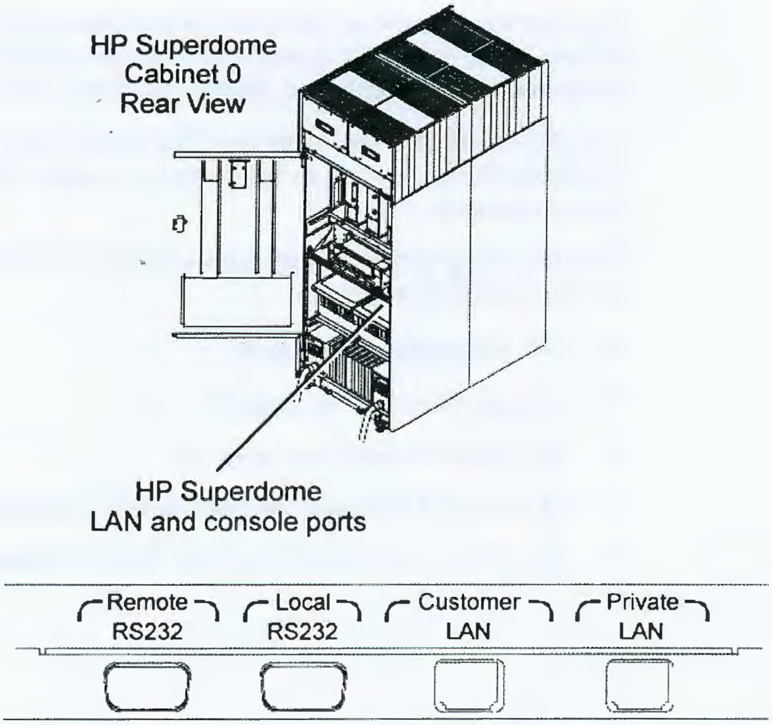


5738

Service Processor for HP Superdome

On HP Superdome servers, service processor functionality is provided by the “GSP UGUY and SUB” cabinet hardware, which can be seen in the rear of the cabinet above the LAN and console ports (see Figure 1-14). Use the *cabinet 0 (not cabinet 1) LAN and RS-232 connections* to access the service processor. The cabinet 0 “Customer LAN” port provides remote telnet access to the service processor. A direct RS-232 serial connection to the service processor is available through the “Local RS232” port. The “Remote RS232” port is for external, remote modem access to the service processor.

Figure 1-14 **HP Superdome Service Processor LAN and Serial Ports**



Overview of nPartitions

On HP's nPartition servers, each **nPartition** is a “logical system” that has its own dedicated portion of the server hardware that can run a single instance of the HP-UX 11i operating system. Each nPartition can boot, reboot, and operate independently of any other nPartitions and hardware within the same server complex.

Each nPartition has one or more **cells** (containing processors and memory) that are assigned to the nPartition for its exclusive use. Any **I/O chassis** that is attached to a cell belonging to an nPartition also is assigned to the nPartition. (Each chassis has PCI card slots plus any I/O cards and attached devices, and may also have **core I/O**.)

The **server complex** includes all hardware within an nPartition server: all cabinets, cells, I/O chassis, I/O devices and racks, management and interconnecting hardware, power supplies, and fans.

You can configure one or more nPartitions within a server complex, allowing the hardware to function as a single HP-UX 11i system or as many systems.

The following concepts and issues related to nPartitions are introduced in the rest of this section:

- *Cell Properties* on page 61
- *Genesis Partition* on page 63
- *Partition Numbers* on page 64
- *nPartition Local and Remote Access* on page 64
- *nPartition Active and Inactive States* on page 66

5736

Cell Properties

Cells in an HP nPartition server have various properties that determine how the cells can be used and managed.

The cell properties discussed here include: *Assigned and Unassigned Cells*, *Base Cells*, *Core Cells*, and *Active and Inactive Cells*.

To list details about all cells in a server complex, you can use the `parstatus -C` HP-UX command or Partition Manager.

The `parstatus -C` command output includes the current nPartition assignments, usage, and I/O details for the cells.

```
# parstatus -C
[Cell]
                        CPU     Memory                                 Use
                        OK/     (GB)                           Core    On
Hardware   Actual       Deconf/ OK/                            Cell    Next Par
Location   Usage        Max     Deconf    Connected To         Capable Boot Num
========== ============ ======= ========= =================== ======= ==== ===
cab0,cell0 active core  4/0/4    8.0/ 0.0 cab 0,bay0,chassis1 yes     yes  0
cab0,cell1 active base  4/0/4    8.0/ 0.0 -                   no      yes  0
cab0,cell2 active base  4/0/4    8.0/ 0.0 cab 0,bay1,chassis3 yes     yes  0
cab0,cell3 absent       -       -         -                   -       -    -
cab0,cell4 active core  2/0/4    4.0/ 0.0 cab 0,bay0,chassis3 yes     yes  1
cab0,cell5 active base  2/0/4    4.0/ 0.0 -                   no      yes  1
cab0,cell6 active base  2/0/4    4.0/ 0.0 cab 0,bay1,chassis1 yes     yes  1
cab0,cell7 absent       -       -         -                   -       -    -

#
```

Assigned and Unassigned Cells

Each cell in an nPartition server complex either is *assigned* to one of the nPartitions in the complex, or it is *unassigned* and thus is not used by any of the nPartitions. If an I/O chassis is attached to an unassigned cell, then the chassis likewise is not assigned to an nPartition.

Cells that are unassigned are considered to be available resources; they are on the server complex's "free cell list" and are free to be assigned to any of the existing nPartitions, or can be used to create new nPartitions.

Base Cells

For the HP-UX 11i release, all cells within an Partition are **base cells.**

The HP-UX 11i utilities for managing nPartitions automatically set the cell type to base cell, if you do not specify the cell type.

Core Cells

One cell in each nPartition must serve as the **active core cell**. The core cell is a cell that is connected to an I/O chassis that has **core I/O**. The core cell controls the nPartition until HP-UX has booted, and it provides console access for the nPartition.

The core cell's core I/O provides console access for the nPartition through the service processor (GSP or MP).

The monarch processor on the core cell runs the Boot Console Handler (BCH) code while all other processors are idle until HP-UX is booted.

Although an nPartition can have multiple **core-capable cells** (any assigned cell that has an I/O chassis with core I/O), only one core I/O is actively used in an nPartition (the one belonging to the active core cell).

To be *eligible* as a core cell, a cell must be assigned to the nPartition, it must be active, and it must be attached to an I/O chassis containing functional core I/O.

The core cell is selected by system firmware in the early stages of the nPartition boot process.

By default—on HP Superdome and HP rp8400 servers—the lowest numbered eligible cell in an nPartition is selected as the core cell.

By default on HP rp7405/rp7410 servers only, cell 1 is selected as the core cell if it is eligible.

You can define up to four **core cell choices (or "alternates")** for an nPartition (two core-capable cells are currently supported on HP rp7405/rp7410 and HP rp8400 servers). The core cell choices are cells that you prefer to be selected as the nPartition's core cell. If your first core cell alternate cannot be used, then the second choice is checked; if the second choice fails, then any other choices are tried, in the order you specified.

When none of the core cell choices can serve as the active core cell, the nPartition then attempts to select an eligible cell using the default process.

Active and Inactive Cells

Cells that are assigned to an nPartition and have booted to form an nPartition are **active cells** whose resources (processors, memory, and any attached I/O) can be actively used by software running in the nPartition.

5734

Cells that are **inactive** either are not assigned to an nPartition, or they have not participated in *partition rendezvous* to form an nPartition with any other cells assigned to the nPartition. (Partition rendezvous is the point during the nPartition boot process when all available cells in an nPartition join together to establish which cells are active for the current boot of the nPartition.)

For example, a cell can be inactive when it is powered off, has booted with a "n" use-on-next-boot value, or is assigned to an nPartition that has been reset to the ready for reconfig state.

The resources belonging to inactive cells are not actively used by an nPartition. For a cell's resources to be actively used the cell must boot and participate in partition rendezvous.

Genesis Partition

The **Genesis partition** is the initial, one-cell nPartition created within a server complex. The Genesis partition is *just like any other nPartition* except in how it is created.

If your server complex has its nPartitions pre-configured by HP, you do not need to create a Genesis partition.

However, you always have the option of creating a Genesis partition by using the service processor (GSP or MP) Command menu's `CC` command, `G` option, to "wipe out" any existing nPartition definitions and start a new complex configuration that includes only the Genesis partition.

You can use HP-UX utilities running on the Genesis partition as the method for configuring all nPartitions in the complex. The Genesis partition always is partition number 0.

When it is first created, the Genesis partition consists of one cell that is connected to an I/O chassis that has core I/O installed. The Genesis partition also should have a bootable disk (or a disk onto which you can install HP-UX).

If HP-UX is not installed on the Genesis partition's disk(s), you can boot the Genesis partition to the Boot Console Handler (BCH) menu and from that point install HP-UX. This installation requires either having access to an HP-UX install server, or a CD-ROM drive (or DVD-ROM drive) connected to the cell's I/O chassis.

After you boot HP-UX on the Genesis partition, you can modify the nPartition to include additional cells. You also can create other, new nPartitions and can modify them from the Genesis partition or from any other nPartition running HP-UX.

Note that—once you create additional nPartitions—you do not necessarily have to use the Genesis partition to perform your nPartition management and configuration tasks.

Partition Numbers

Each nPartition has its own unique **partition number** that the nPartition commands and utilities use for identifying the nPartition.

When you create an nPartition, the utility you use assigns the nPartition the lowest available partition number. For example, the Genesis partition always is partition number 0 because it is the first and only nPartition in the server complex when it is created, and the second nPartition to be created is partition number 1.

After you remove an nPartition, no cells are assigned to the nPartition. As a result, the nPartition tools can assign cells to the partition number when creating a new nPartition.

For example, if you remove partition number 2, then the `parcreate` command or Partition Manager tool can assign cells to partition number 2 when creating a new nPartition, if all lower-numbered nPartitions (partition numbers 0 and 1) already are defined.

nPartition Local and Remote Access

Your access to an nPartition—whether local or remote—determines your ability to configure and manage the nPartition. Some capabilities require *local* partition access while other capabilities only require that you login to *any* of the nPartitions in the server complex, including remote partitions.

Local nPartition

When you login to HP-UX running on an nPartition, or when you access an nPartition's BCH interface or console, the nPartition you are accessing is considered to be the **local nPartition**.

5732

Remote nPartition

All nPartitions in the complex *other than the one you are accessing* are considered to be **remote nPartitions**.

You can use the `parstatus -w` command to list the partition number for the local nPartition.

```
# parstatus -w
The local partition number is 1.
# parstatus -P
[Partition]
Par                 # of  # of I/O
Num Status          Cells Chassis  Core cell  Partition Name (first 30 chars)
=== ============    ===== ======== ========== ===============================
 0  active            2       2    cab0,cell0 feshd2
 1  active            1       1    cab1,cell2 feshd5
#
```

Tools Requirements and Limits for Use in Local and Remote nPartitions

The following list describes many of the administration requirements for using HP-UX tools on a local or remote nPartition. For detailed procedures, refer to these chapters: *Booting and Resetting nPartitions* on page 197, *Managing nPartitions* on page 243, and *Listing and Managing Server Hardware* on page 305.

- **Listing Information**—You can use the `parstatus` command or the Partition Manager utility from *any* nPartition to list nPartition and complex information.
- **Adding (Assigning) a Cell** to an nPartition—You can use `parmodify` or Partition Manager from *any* nPartition to assign a cell to any nPartition in the server complex.
- **Removing (Unassigning) a Cell** from an nPartition—You can unassign an *inactive cell* from its nPartition by using `parmodify` or Partition Manager on any nPartition. However, to unassign an *active cell* you must use these tools from the *local* nPartition (the nPartition to which the cell is assigned).
- **Powering On or Off a Cell**—To power on or off a cell that is *unassigned*, you can use `frupower` or Partition Manager on any nPartition. To power on or off an *assigned cell*, the cell must be *inactive* and you must use `frupower` or Partition Manager from the *local* nPartition (the nPartition to which the cell is assigned).

- **Rebooting or Shutting Down HP-UX**—To reboot or shut down HP-UX you must issue the `/usr/sbin/shutdown` command and appropriate options (such as `-r`, `-R`, `-h`, `-R -H`, or others) from the *local* nPartition.
- **Turning Attention Indicators (LEDs) On or Off**—You can use the `fruled` command or Partition Manager to control the attention indicators for all hardware in the server complex from *any* nPartition.

nPartition Active and Inactive States

Each nPartition's boot state either is *active* or *inactive*.

Active nPartition

An nPartition that is **active** has at least one cell that is active (not in a boot-is-blocked state). When an nPartition is active, the nPartition's available cells complete partition rendezvous and then the Boot Console Handler (BCH) interface is loaded and is displayed on the nPartition's console. HP-UX is loaded and run from BCH on an active partition.

Inactive nPartition

An **inactive partition** is considered to be in the **ready for reconfig** state, because all cells assigned to the nPartition either remain at a boot-is-blocked state or are powered off.

Use the `parstatus -P` HP-UX command to list all nPartitions and their boot states (active or inactive).

```
# parstatus -P
[Partition]
Par                # of  # of I/O
Num Status         Cells Chassis  Core cell  Partition Name (first 30 chars)
=== ============ ===== ======== ========== ===============================
 0  inactive       2       1     ?          feshd5a
 1  active         2       1     cab1,cell2 feshd5b
#
```

To make an inactive partition *active*, use the service processor (GSP or MP) Command menu's `BO` command. The `BO` command clears the boot-is-blocked flag for all cells assigned to the nPartition, thus allowing the cells to rendezvous and enabling the nPartition to run the BCH interface. (If all of an nPartition's cells are powered off, you must power on its cells to enable the nPartition to become active.)

5730

To make a partition *inactive*, you can issue commands from HP-UX, the BCH interface, or the service processor (GSP or MP) Command menu.

- When HP-UX is running on an nPartition, you can make the nPartition inactive by issuing the `shutdown -R -H` command to shut down HP-UX, reboot all cells, and hold all cells at a boot-is-blocked state.
- When the BCH interface is available for an nPartition, you can make the nPartition inactive by issuing the BCH interface's `RECONFIGRESET` command. This reboots all cells assigned to the nPartition and holds all cells at a boot-is-blocked state.
- If an nPartition is active but is not responsive (that is, if you can neither login as root to issue the `shutdown -R -H` command nor access the nPartition's BCH interface from its console), then use the service processor Command menu's `RR` command to make the nPartition inactive. This reboots all cells assigned to the nPartition and holds all cells at a boot-is-blocked state.

CAUTION Issuing the service processor Command menu's `RR` command immediately halts all processing and I/O activity on the specified nPartition. Be certain to *correctly specify* which nPartition is to be reset to the ready for reconfig state.

All three methods above reboot an nPartition and hold all of its cells at boot-is-blocked; as a result the rebooted nPartition is placed in the ready for reconfig (inactive) state.

5729

Complex Profiles

Each HP nPartition server's **Complex Profile** includes the data that determine how the server's hardware is assigned to and used by nPartitions.

When you configure nPartitions and modify nPartition settings, the commands and utilities you use lock and unlock the server's Complex Profile when revising it.

The Complex Profile consists of two parts: *Stable Complex Configuration Data* (complex-wide settings) and *Partition Configuration Data* (individual nPartition settings).

You can modify nPartition configurations (and thus revise the Complex Profile) by using the server's service processor Command menu, nPartition Boot Console Handler (BCH) interfaces, or HP-UX nPartition commands and Partition Manager.

Each Complex Profile contains the following information for the server complex.

- **Stable Complex Configuration Data**

  This portion of the Complex Profile stores complex-wide information, including the following details:

  — The name of the complex

  — Which cells are assigned to which nPartitions, and which cells are unassigned (those on the free cell list, which are available to be assigned to any nPartition)

  — The model number, model string, product numbers, and the serial number for the complex

  The server complex's service processor stores the master copy of the Stable Complex Configuration Data. Each cell also stores a copy if this data.

- **Partition Configuration Data**

  This portion of the Complex Profile stores nPartition-specific information.

5728

The Partition Configuration Data includes the following details for each nPartition in the server complex:

- The nPartition's name, number, and IP address
- The PRI, HAA, and ALT boot paths and boot actions (path flags)
- The use-on-next-boot setting for each cell

  This determines whether the cell is allowed to become active and join (rendezvous) the rest of the cells in the nPartition.
- The core cell choices

  This is a list of any cells that are preferred to be selected as the nPartition's active core cell.

Each nPartition has its own Partition Configuration Data, a copy of which is stored on each cell in the nPartition. The server's service processor also stores copies of this data for all nPartitions.

The server's service processor manages all Complex Profile data and keeps all copies of the data coherent.

Complex Profile Locks

Locking and unlocking Complex Profiles is automatically managed by the commands and utilities that you use to configure and modify nPartitions. Portions of the Complex Profile data are updated when you modify nPartition configurations or server complex configurations. For more details on nPartition reconfiguration, including procedures for manually unlocking complex profiles, refer to the chapter *Managing nPartitions* on page 243.

5727
28

Tools for Managing nPartitions

You can use several different software tools to create, modify, and monitor a server's nPartitions and related server complex hardware.

These tools have capabilities that overlap in some cases, but each tool also has unique features and access requirements.

The tools for managing nPartitions are:

- Service Processor (GSP or MP) menus
- Virtual Front Panel (VFP) interfaces
- Boot Console Handler (BCH) interfaces
- HP-UX nPartition Configuration Commands
- Partition Manager (`/opt/parmgr/bin/parmgr`)
- System Administration Manager (SAM, `/usr/sbin/sam`)

NOTE

The service processor in HP servers is sometimes called the Management Processor (MP) and sometimes the Guardian Service Processor (GSP).

Regardless of the name, the service processor in these servers provides approximately the same features and performs essentially the same role.

Throughout this document, the term "service processor" refers to both the MP and GSP service processors.

Table 1-3 lists the nPartition management tools and describes each tool's features and capabilities.

Use Table 1-3 to select the most appropriate nPartition management tool based on the tasks you need to perform and the ways in which you can access the system.

Table 1-3 **Management Tools for nPartitions**

Partition Tool	Features and Restrictions
Service Processor (GSP or MP) menus	The service processor menus provide a complex-wide service interface that allows access to complex hardware and nPartitions defined within the complex. Also refer to the chapter *Using Console and Service Processor Interfaces* on page 125 for details. • Availability—Using service processor menus requires logging in to the service processor. Your service processor login account determines your level of access to the complex hardware and nPartitions. • Features—Service processor commands, access to nPartition consoles, Virtual Front Panels (VFPs) for live nPartition status details, ability to power cycle hardware, ability to reset and TOC nPartitions, ability to view live chassis codes, and access to console and chassis code log files. • Tasks Supported—Monitoring and listing status for all nPartitions and hardware within a server complex. Viewing chassis codes. nPartition console access. nPartition reset and complex hardware power control.
Virtual Front Panel (VFP) interfaces	The VFP interface provides a real-time display of nPartition and cell *boot states* and *activities*. Also refer to the chapter *Using Console and Service Processor Interfaces* on page 125 for details. • Availability—Viewing the VFP interface for an nPartition (or entire system) requires logging in to the service processor. Your service processor user account determines which nPartition VFPs you can access. • Features—Real-time text summaries of nPartition and cell boot states and activities. • Tasks Supported—Monitoring nPartition boot progress and associated cell status.

5725

Table 1-3 Management Tools for nPartitions (Continued)

Partition Tool	Features and Restrictions
Boot Console Handler (BCH) interface	The BCH interface is the method for interacting with an nPartition before it has booted HP-UX. Each nPartition's BCH interface provides menus for configuring nPartition settings and booting HP-UX. Also refer to the chapter *Using Console and Service Processor Interfaces* on page 125 for details. • Availability—Using an nPartition's BCH interface requires accessing the nPartition's console through the service processor Console menu. • Features—Allows you to select which device and which HP-UX kernel is booted, to configure the *boot actions* for devices, and to software-deallocate CPUs, memory, and cells. • Tasks Supported—Configuring and managing the HP-UX boot process, getting nPartition-specific information, resetting the local nPartition, configuring various nPartition settings.
HP-UX nPartition Configuration Commands	The HP-UX nPartition configuration commands allow you to configure, modify, and monitor nPartitions and hardware within a server complex. See the section *Using HP-UX nPartition Configuration Commands* on page 85 for details. The commands include `parcreate`, `parmodify`, `parstatus`, `parremove`, `parunlock`, `fruled`, and `frupower`. • Availability—Using the HP-UX nPartition configuration commands requires logging in to HP-UX running on an nPartition. All users can issue the `parstatus` and `fruled` commands, but all other commands require `root` user permissions. • Features—These commands allow you to manage nPartitions and hardware when HP-UX is in single– or multi-user mode and when you are logged in with text-only terminal access. • Tasks Supported—Configuring, modifying, and getting information about nPartitions and hardware within a server complex.

5924

21

Table 1-3 Management Tools for nPartitions (Continued)

Partition Tool	Features and Restrictions
Partition Manager (parmgr)	Partition Manager (/opt/parmgr/bin/parmgr) provides a graphical interface for configuring, modifying, and managing nPartitions and hardware within a server complex. See the section *Using the Partition Manager Utility* on page 106 for details. • Availability—You can use Partition Manager when HP-UX is running in multi-user mode on the nPartition. You can use Partition Manager as a stand-alone X window application (parmgr) and can launch it from SAM. Partition Manager also can be launched from a PC Web browser. • Features—Provides a graphical user interface and also supports Web console access. Performs additional error checking beyond what the HP-UX nPartition configuration commands support. Also supports I/O card online addition and replacement. • Tasks Supported—Configuring, modifying, and getting information about nPartitions and hardware within a hard-partitionable server complex. • Detailed Information—See the parmgr online help.
System Administration Manager (SAM)	When using SAM (/usr/sbin/sam) in graphical mode, you can launch Partition Manager from SAM. See Partition Manager, above, for details.

523

HP-UX 11i Release Features

The *HP-UX 11i June 2003 Release Notes* lists the latest feature additions and changes to HP-UX operating system and the various “operating environment” bundles.

Each of the HP-UX operating environment bundles includes its own collection of applications. You can install any *one* of the operating environments at a time.

Use the **`swlist -l bundle`** command to list all installed software bundles, including operating environments.

The *Read Before Installing or Updating HP-UX 11i, June 2003* booklet, which is distributed with HP-UX media, also has current details on release and operating environment features.

The release notes and “Read Before” booklet also are available on the **`http://docs.hp.com/`** Web site.

The HP-UX 11i operating environments are described in the following list.

- HP-UX 11i Operating Environment

  This is an integrated and tested software solution for servers. It contains the base HP-UX 11i operating system and selected drivers and applications.

- HP-UX 11i Enterprise Operating Environment

  This is an operating environment marketed and supported only for commercial servers. It contains everything in the basic HP-UX 11i Operating Environment plus additional applications.

- HP-UX 11i Mission Critical Operating Environment

  This is an operating environment marketed and supported only for commercial servers. It contains everything in the HP-UX 11i Enterprise Operating Environment plus additional applications.

- HP-UX 11i Technical Computing Environment

  This is an operating environment marketed and supported for technical computing servers and workstations. It contains the base HP-UX 11i operating system and selected drivers and applications.

5322

- HP-UX 11i Minimal Technical Operating

  This is an operating environment defined for HP workstations. It contains all the base functionality. However, compared to the Technical Computing Operating Environment, the set of additional applications is greatly reduced.

HP-UX Hardware Paths for nPartitions

The HP-UX hardware path for nPartition systems is provided in the format described here.

The `/usr/sbin/ioscan` HP-UX command reports the hardware path for active components within the nPartition in which the command is issued.

You also can use the `/usr/bin/rad -q` command to list details about active I/O slots and cards in the local nPartition.

NOTE The `ioscan` and `rad` commands only report information about the *currently active* hardware components *in the local partition.*

These commands do not report details for hardware that is not assigned to the local nPartition or hardware that is inactive in the nPartition.

Hardware Paths in nPartitions

The components of nPartition hardware paths are:

`a/b/c/d/e.f.g`

where these components are as described in the following list.

- `a`

  Is the global cell number.

- `b`

  Is a processor (10–13), memory (5), or a system bus adapter (0). Each I/O chassis has a single system bus adapter.

- `c`

  Is a local bus adapter (the *LBA*, one for each PCI card slot in the chassis). The LBA connects its corresponding PCI card slot with the system bus adapter.

NOTE The LBA number *is not necessarily the same* as the PCI slot number.

S720

Use the rad -q command to list all active PCI slots in an nPartition along with their corresponding hardware paths. See *PCI Card Slot and Hardware Path Numbering* on page 79.

- d

  Is the card's address on the slot's PCI bus.

  Typically this is 0 (zero), although the core I/O card has multiple devices and addresses in a single card.

- e

  Is the function for the I/O card. Typically this is 0 (zero) for single-function cards.

- f

  Is the target of the I/O device, or SCSI ID.

- g

  Is a device-specific address such as a SCSI controller (initiator).

See the *ioscan* (1M) manpage for details on using ioscan to list hardware path information.

Example 1-1 **ioscan Output for a One-Cell HP Superdome nPartition**

The following example shows ioscan output for a one-cell nPartition.

In this example, the hardware path for the cell is 12, indicating that the cell is in slot 4 in cabinet 1. See *Specifying Cells and I/O Chassis to Commands* on page 87 for details about cell path formats.

```
# ioscan
H/W Path          Class                        Description
=======================================================
                  root
12                cell
12/0                  ioa                      System Bus Adapter (804)
12/0/0                   ba                    Local PCI Bus Adapter (782)
12/0/0/0/0                     tty             PCI Serial (103c1048)
12/0/0/1/0                     lan             HP PCI 10/100Base-TX Core
12/0/1                   ba                    Local PCI Bus Adapter (782)
12/0/2                   ba                    Local PCI Bus Adapter (782)
12/0/3                   ba                    Local PCI Bus Adapter (782)
12/0/4                   ba                    Local PCI Bus Adapter (782)
```

```
12/0/6                 ba                    Local PCI Bus Adapter (782)
12/0/6/0/0                   ext_bus         SCSI C87x Ultra Wide Differential
12/0/6/0/0.5                    target
12/0/6/0/0.5.0                     disk      SEAGATE ST39173WC
12/0/6/0/0.6                    target
12/0/6/0/0.6.0                     disk      SEAGATE ST39173WC
12/0/6/0/0.7                    target
12/0/6/0/0.7.0                     ctl       Initiator
12/0/8                 ba                    Local PCI Bus Adapter (782)
12/0/9                 ba                    Local PCI Bus Adapter (782)
12/0/10                ba                    Local PCI Bus Adapter (782)
12/0/11                ba                    Local PCI Bus Adapter (782)
12/0/12                ba                    Local PCI Bus Adapter (782)
12/0/14                ba                    Local PCI Bus Adapter (782)
12/5                memory                   Memory
12/10               processor                Processor
12/11               processor                Processor
12/12               processor                Processor
12/13               processor                Processor
#
```

PCI Card Slot and Hardware Path Numbering

On nPartition servers, the PCI card slot numbers (within an I/O chassis) are not necessarily the same as their *local bus adapter* (LBA) number, such as is reported by the `ioscan` or `rad` HP-UX commands.

Table 1-4 shows the correlations among PCI slots and their LBA numbers.

Table 1-4 I/O Numbering: PCI slots and Busses (LBAs)

PCI Card Slot	HP Superdome LBA Number	HP rp8400 and HP rp7405/rp7410 LBA Number
0	0	0
1	1	8
2	2	10
3	3	12
4	4	14
5	6	6
6	14	4
7	12	2
8	11	1
9	10	—
10	9	—
11	8	—

The **`rad -q`** command lists each active PCI slot, its associated HP-UX hardware path, and other slot details.

The **`ioscan -C ba`** command lists the active PCI slots ("Local PCI Bus Adapter") for your nPartition.

The order in which `ioscan` reports the PCI slots (in LBA number order) *does not* correspond to the order in which the slots physically are arranged (PCI card slot order, left-to-right or right-to-left).

5716
21

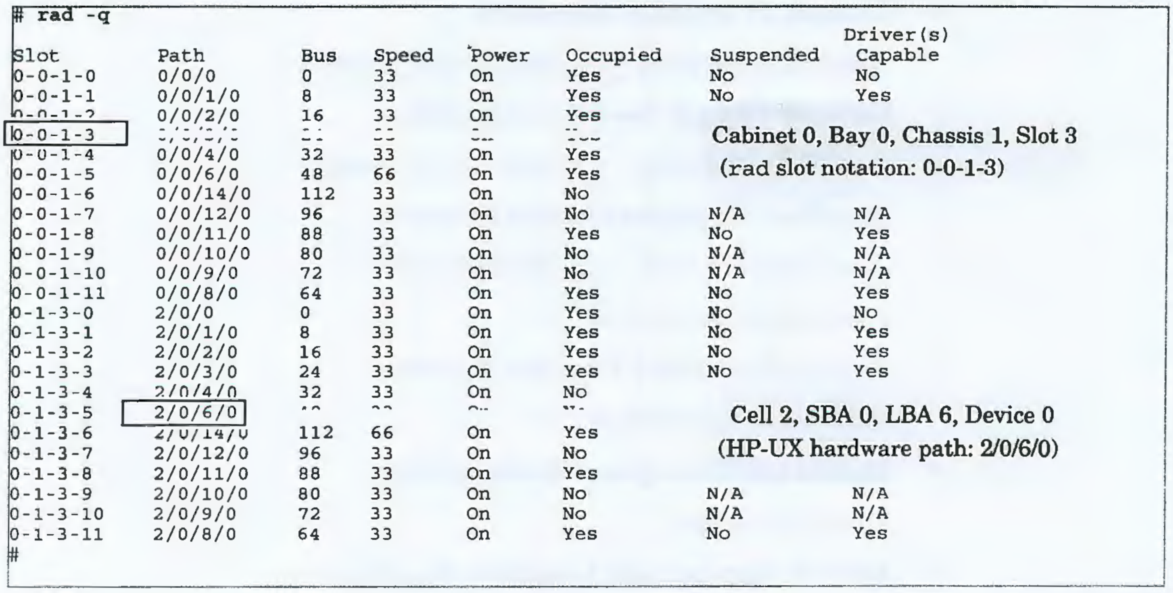
rad Command Output in nPartitions

This section covers the rad command's output on nPartitions. For complete details, see the *rad* (1M) manpage.

NOTE When adding or replacing I/O cards, use the SAM (/usr/sbin/sam) procedures when possible rather than equivalent rad command procedures.

See also the *sam* (1M) and *rad* (1M) manpages.

On HP nPartition servers, the rad command reports PCI card slot details as shown in the following example output. The rad command reports each available PCI slot (*cabinet-bay-chassis-slot*), its corresponding HP-UX hardware path (*cell/sba/lba/device*), and more details.



```
# rad -q
                                                                   Driver(s)
Slot        Path        Bus    Speed   Power   Occupied   Suspended   Capable
0-0-1-0     0/0/0       0      33      On      Yes        No          No
0-0-1-1     0/0/1/0     8      33      On      Yes        No          Yes
0-0-1-2     0/0/2/0     16     33      On      Yes
0-0-1-3     0/0/3/0     24     33      On      Yes
0-0-1-4     0/0/4/0     32     33      On      Yes
0-0-1-5     0/0/6/0     48     66      On      Yes
0-0-1-6     0/0/14/0    112    33      On      No
0-0-1-7     0/0/12/0    96     33      On      No         N/A         N/A
0-0-1-8     0/0/11/0    88     33      On      Yes        No          Yes
0-0-1-9     0/0/10/0    80     33      On      No         N/A         N/A
0-0-1-10    0/0/9/0     72     33      On      No         N/A         N/A
0-0-1-11    0/0/8/0     64     33      On      Yes        No          Yes
0-1-3-0     2/0/0       0      33      On      Yes        No          No
0-1-3-1     2/0/1/0     8      33      On      Yes        No          Yes
0-1-3-2     2/0/2/0     16     33      On      Yes        No          Yes
0-1-3-3     2/0/3/0     24     33      On      Yes        No          Yes
0-1-3-4     2/0/4/0     32     33      On      No
0-1-3-5     2/0/6/0     48     33      On      No
0-1-3-6     2/0/14/0    112    66      On      Yes
0-1-3-7     2/0/12/0    96     33      On      No
0-1-3-8     2/0/11/0    88     33      On      Yes
0-1-3-9     2/0/10/0    80     33      On      No         N/A         N/A
0-1-3-10    2/0/9/0     72     33      On      No         N/A         N/A
0-1-3-11    2/0/8/0     64     33      On      Yes        No          Yes
#
```

Cabinet 0, Bay 0, Chassis 1, Slot 3
(rad slot notation: 0-0-1-3)

Cell 2, SBA 0, LBA 6, Device 0
(HP-UX hardware path: 2/0/6/0)

The rad command only lists slots in PCI chassis that are assigned to the local nPartition and are active.

Licensing Information: Getting Product Details

When you license a software product to run on an HP system, you may need to provide machine or system details to the software vendor as part of the software registration process.

This section describes how to obtain information you may need when licensing non-HP software to run on an HP nPartition server.

For complete information about software product licensing, refer to the company that manufactures or sells the software you plan to use.

To license software for use on HP-UX running on an nPartition, you may need to provide the following details about the nPartition or its server complex:

- **Unique Machine (Complex) Identifier**

  `/usr/bin/getconf _CS_MACHINE_IDENT`

- **Unique nPartition Identifier**

  `/usr/bin/getconf _CS_PARTITION_IDENT`

- **Unique Virtual Partition Identifier**

  `/usr/bin/getconf _CS_PARTITION_IDENT`

- **Machine (Complex) Serial Number**

  `/usr/bin/getconf _CS_MACHINE_SERIAL`

  `/usr/sbin/parstatus -X`

- **Server (Complex) Product Number**

  `/usr/sbin/parstatus -X`

- **Hardware (Complex) Model String**

  `/usr/bin/model`

- **HP-UX Version and Installed Bundles**

  For the HP-UX version: `/usr/bin/uname -r`

  For all bundles installed: `/usr/sbin/swlist -l bundle`

5714

nPartition and Virtual Partition Unique Identifiers

NOTE Use the getconf command or the confstr() call to obtain unique identifiers. Do not use the uname -i command, which *does not report unique IDs* for nPartition systems.

In order to guarantee compatibility on current and future platforms, use the interfaces to *getconf* (1) and *confstr* (3C) to retrieve unique machine identifiers.

The interfaces include the _CS_PARTITION_IDENT and _CS_MACHINE_IDENT parameters:

- For a *nPartition-specific* or a *virtual partition-specific* unique ID use this command:

  /usr/bin/getconf _CS_PARTITION_IDENT

  The unique partition identifier value for a virtual partition environment has virtual partition-specific data added that does not appear for an equivalent non-vPars environment. See the examples that follow.

- For a *complex-specific* unique ID use this command:

  /usr/bin/getconf _CS_MACHINE_IDENT

On HP PA-RISC nPartition servers, the complex, nPartition, and virtual partition unique IDs are based in part on the machine serial number.

To retrieve the machine serial through these interfaces, specify the _CS_MACHINE_SERIAL parameter to them.

See the *confstr* (3C) manpage for details on these parameters and their use.

Example 1-2 **Unique IDs for an nPartition and Complex**

The following examples show nPartition-unique and complex-unique IDs returned by the getconf command, as well as the local nPartition number and machine serial number.

```
# parstatus -w
The local partition number is 1.
# /usr/bin/getconf _CS_PARTITION_IDENT
Z3e02955673f9f7c9_P1
```

```
# /usr/bin/getconf _CS_MACHINE_IDENT
Z3e02955673f9f7c9
# /usr/bin/getconf _CS_MACHINE_SERIAL
USR2024FP1
#
```

Example 1-3 Unique IDs for Virtual Partitions (vPars)

The following example shows the virtual partition-unique ID returned by the getconf command, as well as the local nPartition number and the current virtual partition's name.

```
# parstatus -w
The local partition number is 0.
# vparstatus -w
The current virtual partition is Shad.
# getconf _CS_PARTITION_IDENT
Z3e0ec8e078cd3c7b_P0_V00
#
```

For details on virtual partitions, refer to the chapter *Virtual Partitions (vPars) Management on nPartitions* on page 441.

5312

Using HP-UX nPartition Configuration Commands

HP-UX 11i provides you with several HP-UX commands for configuring and managing nPartitions and related server hardware.

The nPartition commands include: `parcreate`, `parmodify`, `parremove`, `parstatus`, `parunlock`, `fruled`, and `frupower`. Table 1-5 on page 86 describes each of these commands.

Using these commands you can create, modify, monitor, and remove nPartitions; get detailed server hardware information; and manipulate attention indicators (LEDs) and power.

When using these commands, you can specify cells and I/O chassis with the notations shown in *Specifying Cells and I/O Chassis to Commands* on page 87.

NOTE

The HP-UX nPartition configuration commands are supported only on HP servers that support nPartitions.

These commands are supported by HP-UX kernels built with nPartition support enabled (the `hd_fabric` driver), and they use the libfab.1 library.

Table 1-5 describes the nPartition configuration commands and lists sections where you can find each command's syntax and details.

Table 1-5 HP-UX nPartition Configuration Commands

Command	Description
`parcreate`	Create a new nPartition; `root` permission is required. See *parcreate Command* on page 93.
`parmodify`	Modify an existing nPartition; `root` permission is required. See *parmodify Command* on page 95.
`parremove`	Remove an existing nPartition; `root` permission is required. See *parremove Command* on page 98.
`parstatus`	Display nPartition information and hardware details for a server complex. See *parstatus Command* on page 99.
`parunlock`	Unlock Complex Profile data (use this command with caution); `root` permission is required. See *parunlock Command* on page 101.
`fruled`	Blink the attention indicators (LEDs) or turn them off. This command can control these indicators for cells, I/O chassis, and cabinet numbers. See *fruled Command* on page 102.
`frupower`	Display status or turn power on or off for cells and I/O chassis; `root` permission is required. See *frupower Command* on page 104.

5710

Specifying Cells and I/O Chassis to Commands

Use the cell and I/O chassis notation described in this section when you manage, configure, and inquire about cells and I/O chassis using the HP-UX nPartition configuration commands.

Details are in the *Cell Specification Formats* and *I/O Specification Format* sections that follow.

Cell Specification Formats

Use either of the following two formats to specify cells when using the HP-UX nPartition configuration commands: *Global Cell Number Format* or *Cell Hardware Location Format*.

- **Global Cell Number Format**

  The global cell number format is identical to the cells' HP-UX hardware path, as reported by `ioscan`. In global format, each cell is given a single unique number that indicates the cell's relative location in the entire server complex.

Table 1-6 Cell IDs in Global Cell Number Format

Cell Slot	0	1	2	3	4	5	6	7
rp7405/rp7410 Global Format	0	1	—	—	—	—	—	—
rp8400 Global Format	0	1	2	3	—	—	—	—
Superdome Cabinet 0 Global Format	0	1	2	3	4	5	6	7
Superdome Cabinet 1 Global Format	8	9	10	11	12	13	14	15

- **Cell Hardware Location Format**

  In cell hardware location format, each cell is identified using two numbers that specify the *cabinet* and the *cell slot with the cabinet* where the cell resides: *cabinet/slot*.

Table 1-7 Cell IDs in Hardware Location Format

Cell Slot	0	1	2	3	4	5	6	7
rp7405/rp7410 HW Loc Format	0/0	0/1	—	—	—	—	—	—
rp8400 HW Loc Format	0/0	0/1	0/2	0/3	—	—	—	—
Superdome Cabinet 0 HW Loc Format	0/0	0/1	0/2	0/3	0/4	0/5	0/6	0/7
Superdome Cabinet 1 HW Loc Format	1/0	1/1	1/2	1/3	1/4	1/5	1/6	1/7

Both of these cell ID formats specify each cell's precise physical location in a server complex. For example, `parstatus -c9` and `parstatus -c1/1` specify the same cell.

```
# parstatus -c9
[Cell]
                        CPU     Memory                                Use
                        OK/     (GB)                          Core    On
Hardware   Actual       Deconf/ OK/                           Cell    Next Par
Location   Usage        Max     Deconf    Connected To        Capable Boot Num
========== ============ ======= ========= =================== ======= ==== ===
cab1,cell1 active base  4/0/4    8.2/ 0.0 -                   no      yes  1

# parstatus -c1/1
[Cell]
                        CPU     Memory                                Use
                        OK/     (GB)                          Core    On
Hardware   Actual       Deconf/ OK/                           Cell    Next Par
Location   Usage        Max     Deconf    Connected To        Capable Boot Num
========== ============ ======= ========= =================== ======= ==== ===
cab1,cell1 active base  4/0/4    8.2/ 0.0 -                   no      yes  1

#
```

I/O Specification Format

Use the following I/O hardware location format when specifying an I/O chassis to the HP-UX nPartition configuration commands:

cabinet/*bay*/*chassis*

The *cabinet*, *bay*, and *chassis* fields specify the physical location of the I/O chassis. The values of these fields are as follows.

- *cabinet*

  specifies the cabinet number where the I/O chassis resides.

  On HP rp7405/rp7410 and rp8400 servers, the cabinet number always is `0`.

  On HP Superdome servers, the cabinet number can be:

  — `0` — the left Compute cabinet.

  — `1` — the right Compute cabinet, if present.

  — `8` — an I/O Expansion cabinet, if present.

  — `9` — an I/O Expansion cabinet, if present.

- *bay*

  specifies the I/O bay (within a cabinet) where the I/O chassis resides.

  On HP rp8400 and HP rp7405/rp7410 servers, the bay number always is `0`.

  On HP Superdome servers, the bay number can be:

  — `0` — the *front* bay of a Compute cabinet, or the *bottom* bay of an I/O Expansion cabinet.

  — `1` — the *rear* bay of a Compute cabinet, or the *middle* bay of an I/O Expansion cabinet.

  — `2` — the *top* bay in an I/O Expansion cabinet.

- *chassis*

  specifies the I/O chassis (within a bay).

  On HP rp8400 and HP rp7405/rp7410 servers, the chassis number is:

  — `0` — Chassis 0, which connects to cell 0 and is the left chassis as *viewed from the cabinet rear*: the left eight PCI card slots.

- 1 — Chassis 1, which connects to cell 1 and is the right chassis as *viewed from the cabinet rear*: the right eight PCI card slots.

On HP Superdome servers, the chassis number is:

- 1 — Chassis 1, the left chassis in the bay, as viewed when facing the bay/chassis.
- 3 — Chassis 3, the right chassis in the bay, as viewed when facing the bay/chassis.

In HP Superdome servers all chassis are 12-slot I/O chassis, both in Compute cabinets and in I/O Expansion cabinets.

The example below shows the `parstatus` command listing details about two different I/O chassis (cabinet 0/bay 0/chassis 1, and cabinet 0/bay 1/chassis 3).

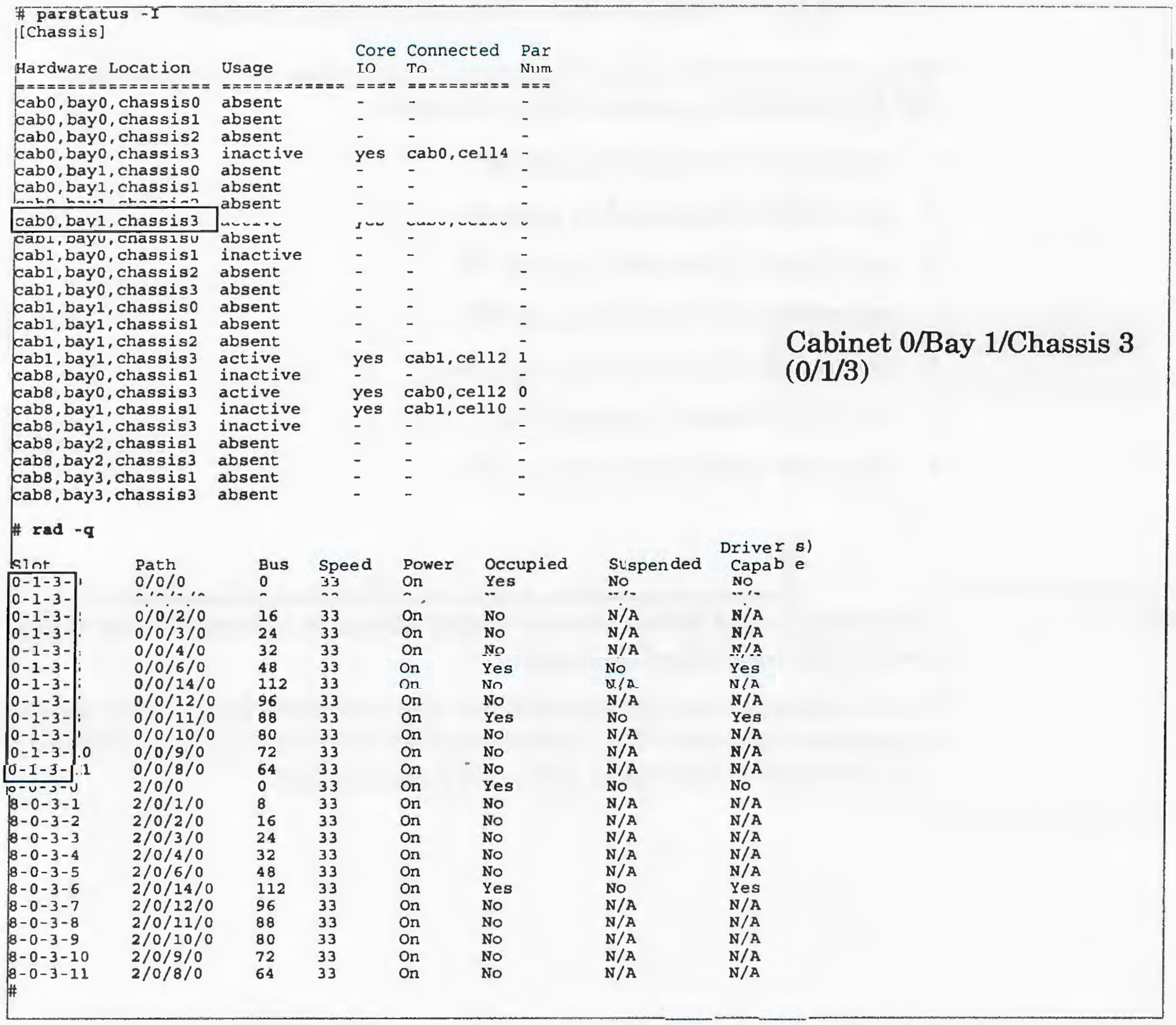
```
# parstatus -i0/0/1
[Chassis]
                                        Core Connected  Par
Hardware Location   Usage               IO   To         Num
=================== ============ ==== ========== ===
cab0,bay0,chassis1  absent              -    -          -

# parstatus -i0/1/3
[Chassis]
                                        Core Connected  Par
Hardware Location   Usage               IO   To         Num
=================== ============ ==== ========== ===
cab0,bay1,chassis3  active              yes  cab0,cell0 0

#
```

Use the `parstatus -I` command to list all I/O chassis within a server complex, regardless of the chassis cell connections and nPartition assignments.

Use the `rad -q` command to list the *currently available* PCI I/O slots in the local nPartition and their status.

In the following example, both the `parstatus` and `rad` commands show details for various chassis and slots, including chassis 0/1/3.

S706
21



```
# parstatus -I
[Chassis]
                                   Core Connected  Par
Hardware Location   Usage          IO   To         Num
=================== ============ ==== ========== ===
cab0,bay0,chassis0  absent         -    -          -
cab0,bay0,chassis1  absent         -    -          -
cab0,bay0,chassis2  absent         -    -          -
cab0,bay0,chassis3  inactive       yes  cab0,cell4 -
cab0,bay1,chassis0  absent         -    -          -
cab0,bay1,chassis1  absent         -    -          -
cab0,bay1,chassis2  absent         -    -          -
cab0,bay1,chassis3  active         yes  cab0,cell0 0
cab1,bay0,chassis0  absent         -    -          -
cab1,bay0,chassis1  inactive       -    -          -
cab1,bay0,chassis2  absent         -    -          -
cab1,bay0,chassis3  absent         -    -          -
cab1,bay1,chassis0  absent         -    -          -
cab1,bay1,chassis1  absent         -    -          -
cab1,bay1,chassis2  absent         -    -          -
cab1,bay1,chassis3  active         yes  cab1,cell2 1
cab8,bay0,chassis1  inactive       -    -          -
cab8,bay0,chassis3  active         yes  cab0,cell2 0
cab8,bay1,chassis1  inactive       yes  cab1,cell0 -
cab8,bay1,chassis3  inactive       -    -          -
cab8,bay2,chassis1  absent         -    -          -
cab8,bay2,chassis3  absent         -    -          -
cab8,bay3,chassis1  absent         -    -          -
cab8,bay3,chassis3  absent         -    -          -

# rad -q
                                                                Driver s)
Slot        Path        Bus   Speed   Power   Occupied   Suspended   Capab e
0-1-3-0     0/0/0       0     33      On      Yes        No          No
0-1-3-1     0/0/1/0     8     33      On      No         N/A         N/A
0-1-3-2     0/0/2/0     16    33      On      No         N/A         N/A
0-1-3-3     0/0/3/0     24    33      On      No         N/A         N/A
0-1-3-4     0/0/4/0     32    33      On      No         N/A         N/A
0-1-3-5     0/0/6/0     48    33      On      Yes        No          Yes
0-1-3-6     0/0/14/0    112   33      On      No         N/A         N/A
0-1-3-7     0/0/12/0    96    33      On      No         N/A         N/A
0-1-3-8     0/0/11/0    88    33      On      Yes        No          Yes
0-1-3-9     0/0/10/0    80    33      On      No         N/A         N/A
0-1-3-10    0/0/9/0     72    33      On      No         N/A         N/A
0-1-3-11    0/0/8/0     64    33      On      No         N/A         N/A
8-0-3-0     2/0/0       0     33      On      Yes        No          No
8-0-3-1     2/0/1/0     8     33      On      No         N/A         N/A
8-0-3-2     2/0/2/0     16    33      On      No         N/A         N/A
8-0-3-3     2/0/3/0     24    33      On      No         N/A         N/A
8-0-3-4     2/0/4/0     32    33      On      No         N/A         N/A
8-0-3-5     2/0/6/0     48    33      On      No         N/A         N/A
8-0-3-6     2/0/14/0    112   33      On      Yes        No          Yes
8-0-3-7     2/0/12/0    96    33      On      No         N/A         N/A
8-0-3-8     2/0/11/0    88    33      On      No         N/A         N/A
8-0-3-9     2/0/10/0    80    33      On      No         N/A         N/A
8-0-3-10    2/0/9/0     72    33      On      No         N/A         N/A
8-0-3-11    2/0/8/0     64    33      On      No         N/A         N/A
#
```

Cabinet 0/Bay 1/Chassis 3
(0/1/3)

nPartition Commands—Details and Syntax

This section has details and command-line syntax for the following HP-UX nPartition configuration commands:

- *parcreate Command* on page 93
- *parmodify Command* on page 95
- *parremove Command* on page 98
- *parstatus Command* on page 99
- *parunlock Command* on page 101
- *fruled Command* on page 102
- *frupower Command* on page 104

NOTE

The sections that follow provide useful reference information for using the HP-UX nPartition commands.

For the most current information for these commands, see their online manpages: *parcreate* (1M), *parmodify* (1M), *parremove* (1M), *parstatus* (1), *parunlock* (1M), *fruled* (1M), and *frupower* (1M).

S7004

parcreate Command

The /usr/sbin/parcreate command creates a new nPartition.

This command assigns the specified cells (and any attached I/O chassis) to an nPartition after removing the cells from the free cell list. This command assigns a number to the new nPartition and returns the partition number of the newly created nPartition.

Root permission is required to use parcreate.

See the *parcreate* (1M) manpage for complete details. Also refer to the section *Creating a New nPartition* on page 260 for procedures and examples.

Synopsis

```
parcreate [-P PartitionName] [-I IPaddress]
-c cell:[cell_type]:[use_on_next_boot]:[failure_usage]
[-c...]
[-b path] [-t path] [-s path] [-r cell] [-r...] [-B] [-k
s_lock]
```

Options

-P *PartitionName*

Specifies the name of the new nPartition.

-I *IPaddress*

Specifies the IP address that should be used by management tools (like SAM) to address this nPartition.

-c *cell*:[*cell_type*]:[*use_on_next_boot*]:[*failure_usage*]

Specifies the cell(s) to be assigned to the nPartition.

- The only valid *cell_type* value is:

base	Base cell (the default).

- The valid *use_on_next_boot* values for cells are:

y	Participate in reboot. (The default.)
n	Do not participate in reboot.

- The only valid *failure_usage* value is:

ri	Reactivate with interleave (the default).

5703

`-b` *path* Specifies the primary (PRI) boot path.

`-t` *path* Specifies the alternate (ALT) boot path.

`-s` *path* Specifies the secondary (HAA) boot path.

`-r` *cell* Specifies the core cell choices. One to four cells can be specified.

`-B` Specifies to boot the nPartition. The default is not to boot the nPartition and leave it in the ready for reconfig state.

S702

parmodify Command

You can use the /usr/sbin/parmodify command to modify the following attributes of an existing nPartition:

Partition name
Cell assignments (add cells or remove cells)
Attributes of existing cells (such as the use-on-next-boot value)
Core cell and core alternate cells
Boot paths (the primary, alternate, and HA alternate paths)

Root permission is required to use this command.

See the *parmodify* (1M) manpage for complete details. Also refer to the chapter *Managing nPartitions* on page 243 for procedures and examples.

Synopsis

```
parmodify -p PartitionNumber
-a cell:[cell_type]:[use_on_next_boot]:[failure_usage]
[-a...] |
-m cell:[cell_type]:[use_on_next_boot]:[failure_usage]
[-m...] | -I IPaddress | -r cell [-r...] | -d cell [-d...] |
-b path | -t path | -s path | -P PartitionName | -B | -k
s_lock:p_lock
```

The -p option is required.

Options

The parmodify command supports the following command-line options.

-p *PartitionNumber*

Specifies the nPartition to be modified. *PartitionNumber* specifies the unique number (integer) assigned to the nPartition. The -p option is required.

Note that you must also to specify any one or more of the following options.

-a *cell*:[*cell_type*]:[*use_on_next_boot*]:[*failure_usage*]

Specifies the cell(s) to be added to the nPartition.

- The valid *cell_type* value is:

base	Base cell. (The default.)

- The valid *use_on_next_boot* values for cells are:

y	Participate in reboot. (The default.)

`n` Do not participate in reboot.

- The only valid *`failure_usage`* value is:

  `ri` Reactivate with interleave (the default).

`-m` *`cell`*`:[`*`cell_type`*`]:[`*`use_on_next_boot`*`]:[`*`failure_usage`*`]`

Modify attributes of a cell already assigned the nPartition.

For details on *`cell_type`*, *`use_on_next_boot`*, and *`failure_usage`* see the `-a` option's descriptions (above).

`-I` *`IPaddress`*

Specifies the IP address that should be used by management tools (like SAM) to address this nPartition.

`-r` *`cell`*

Specifies the core cell and core alternate cells. One to four core cell choices can be specified.

`-d` *`cell`*

Remove the specified cell from the nPartition.

`-b` *`path`*

Specifies the primary (PRI) boot path.

`-t` *`path`*

Specifies the alternate (ALT) boot path.

`-s` *`path`*

Specifies the secondary (HAA) boot path.

`-P` *`PartitionName`*

Specifies the name of the nPartition.

`-B` Specifies whether to boot the nPartition. The default is not to boot.

When you modify an *inactive* nPartition and specify the `-B` option, the nPartition is booted (and becomes active) immediately after it is modified.

S700
20

When you modifying an *active* nPartition and specify the -B option, you must perform a reboot for reconfig of the modified nPartition. You must perform this reboot for reconfig before any other cell assignments can take place in the server complex.

3699

parremove Command

The /usr/sbin/parremove command removes an existing nPartition. This removes all cells from the nPartition and destroys the nPartition definition.

To remove the *local* nPartition (the nPartition from which you issue this command), you must specify the -F option.

To remove a *remote* nPartition, the remote nPartition must be inactive: it must be shut down to the ready for reconfig state or the parremove command will not be able to remove the nPartition.

Root permission is required to run this command.

See the *parremove* (1M) manpage for complete details. Also refer to the section *Removing (Deleting) an nPartition* on page 278 for procedures and examples.

Synopsis

```
parremove -p PartitionNumber [-F]
```

Options

-p *PartitionNumber*

Specifies the nPartition number to be removed.

-F

Forcibly remove the nPartition. If the nPartition is inactive, the nPartition is removed. If the nPartition is active and if it is the local nPartition, the nPartition is removed.

If the nPartition is active but is not the local nPartition, then the nPartition *will not* be removed.

5698

parstatus Command

The /usr/sbin/parstatus command displays information about the nPartitions or hardware within a server complex. If you specify no arguments, parstatus lists information about several of the major components of the server complex.

You can specify an individual entity (cell, I/O chassis, cabinet, or nPartition) to restrict the output to information about that component.

All users can issue this command.

See the *parstatus* (1) manpage for complete details. Also refer to the chapters *Managing nPartitions* on page 243 and *Listing and Managing Server Hardware* on page 305 for procedures and examples.

Synopsis

```
parstatus -s
parstatus -w
parstatus [-X]
parstatus [-A] [-M] -C|-I
parstatus [-M] -B|-P
parstatus [-M] -i IOchassis [-i...]
parstatus [-V|-M] -c cell [-c...]
parstatus [-V|-M] -b cabinet [-b...]
parstatus [-V|-M] -p PartitionNumber [-p...]
```

Options

`-s` Indicate (through parstatus exit status) whether the system is an HP server that supports nPartitions.

`-w` Display the nPartition number for the local nPartition.

`-X` Display the server complex's attributes.

`-A` Only display the available resources in the complex.

`-V` Increase the amount of information displayed.

`-M` Produce output suitable for machine parsing.

`-C` Show information for all the cells in the complex.

`-I` Show information for all I/O chassis in the complex.

`-B` Show information for all cabinets in the complex.

`-P` Show information for all nPartitions in the complex.

`-c` *`cell`*

Show information about the specified cell.

`-i` *`IOchassis`*

Show information about the specified I/O chassis.

`-b` *`cabinet`*

Show information about the specified cabinet.

`-p` *`partition`*

Show information about the specified nPartition.

5696
21

parunlock Command

The /usr/sbin/parunlock command unlocks the Stable Complex Configuration Data or Partition Configuration Data.

Use this command with caution.

Root permission is required to run this command.

See the *parunlock* (1M) manpage for details. Also refer to the section *Unlocking Complex Profiles* on page 303.

Synopsis

```
parunlock [-p PartitionNumber] [-s]

parunlock -A
```

Options

-p *PartitionNumber*

Unlock the Partition Configuration Data of the specified nPartition.

-s — Unlock the Stable Complex Configuration Data.

-A — Unlock the Stable Complex Configuration Data and the Partition Configuration Data of all the nPartitions in the complex.

5695

fruled Command

The /usr/sbin/fruled command *blinks* hardware attention indicators (LEDs) or *turns them off*.

This command can control the cell attention LEDs in all HP nPartition servers, as well as the I/O chassis LEDs on Superdome servers. The fruled command also can *start and stop blinking* the cabinet number LCDs on HP Superdome compute cabinets and I/O expansion cabinets.

See the *fruled* (1) manpage for details. Also refer to the section *Turning Attention Indicators (LEDs) On and Off* on page 323 for procedures and examples.

Synopsis

```
fruled [-f|-o] [-B] -c cell [-c...]
fruled [-f|-o] [-B] -i IOchassis [-i...]
fruled [-f|-o] -b cabinet [-b...]
fruled [-f] -C [-l cabinet] [-l...]
fruled [-f] -I [-l cabinet] [-l...]
```

Options

-f
: Turn off specified attention LED(s). This is the default.

The -f and -o options are mutually exclusive.

-o
: Start blinking the specified attention LED(s). The -o option is unavailable with -C or -I.

-B
: Start or stop blinking the cabinet number LCD of the cabinet that contains the cell or I/O chassis.

The -B option is only available with -c and -i.

-c *cell*

Blink or turn off the specified *cell* attention LED.

cell can be specified either in the local (*cabinet/slot*) or global (*cell_ID*) format.

-i *IOchassis*

Blink or turn off the specified *IOchassis* attention LED.

-b *cabinet*

5694

Start or stop blinking the cabinet number LCD of the specified *cabinet*.

`-C` Turn off all cell attention LEDs.

`-l` *cabinet*

Limit the scope of the `-C` or `-I` option to a given *cabinet*.

5693
28

frupower Command

The /usr/sbin/frupower command turns on, turns off, or displays the current status of power for cells and I/O chassis in nPartition servers.

NOTE

The frupower command (and Partition Manager) permits you to power on or off *inactive* cells and I/O chassis that are assigned to the current nPartition or are not assigned to any nPartition.

See the *frupower* (1M) manpage for details. Also refer to the section *Powering Cells and I/O Chassis On and Off* on page 312 for procedures and examples.

Syntax

```
frupower [ -d | -o | -f ] -c cell [-c...]

frupower [ -d | -o | -f ] -i IOchassis [-i...]

frupower [-d] -C [-l cabinet] [-l...]

frupower [-d] -I [-l cabinet] [-l...]
```

Options

`-d` Display power status of the specified cells or I/O chassis. This is the default.

`-o` Power on the specified cells or I/O chassis.

The -o and -f options are mutually exclusive. The -o and -f options are unavailable with -C and -I.

`-f` Power off the specified cells or I/O chassis.

`-c cell`

The specified *cell* is powered on/off or the power status is displayed.

A *cell* can be specified either in the local (*cabinet/slot*) or global (*cell_ID*) format.

`-i IOchassis`

The specified *IOchassis* is powered on/off or the power status is displayed.

`-C` Display power status of all cells. By default the scope is the entire complex if the -l option is not specified.

5692

-I — Display power status of all I/O chassis. The scope is the entire complex if the -l option is not specified.

-l *cabinet* — Limit the scope of the -C or -I option to the specified *cabinet*.

S691

Using the Partition Manager Utility

The Partition Manager utility (/opt/parmgr/bin/parmgr) provides a graphical user interface for configuring nPartitions and managing resources within a server complex.

This section introduces these topics about Partition Manager: *Partition Manager Primary Window*, *Running Partition Manager*, *Requirements and Limits*, and *Partition Manager Online Help*.

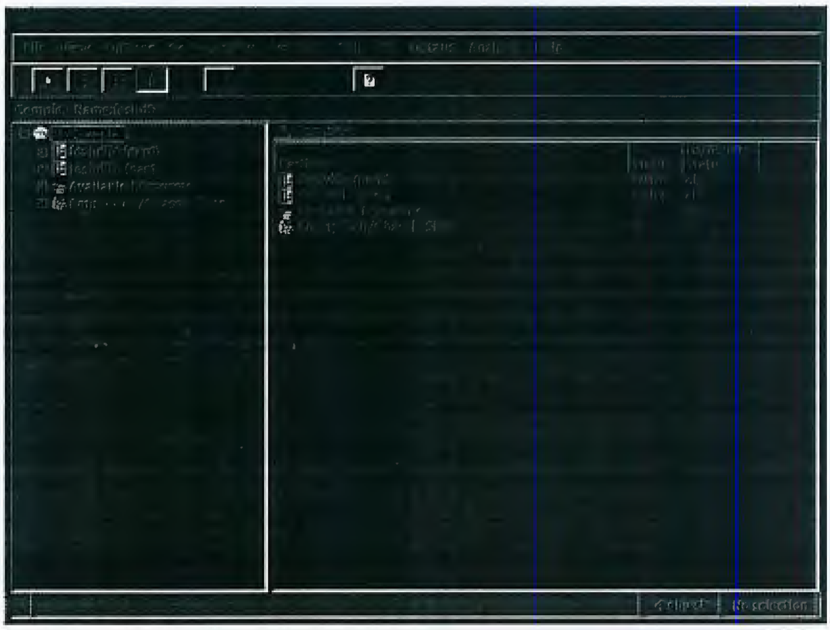
Complete information is in the online help.

Partition Manager Primary Window

The Partition Manager primary window (shown below in Figure 1-15) is the utility's main window for selecting cells, nPartitions, and tasks (menu items).

When you run Partition Manager, by default the program performs an Analyze Complex Health task. If any problems are found, a window reporting those problems is displayed. The primary window is the first window displayed after any complex health analysis results.

Figure 1-15 **Partition Manager Primary Window**



S690
21

The left side of the primary window lists all nPartitions, available resources (installed hardware that is not assigned to an nPartition), and empty cell and I/O chassis slots. Selecting an item on the left side of the primary window displays its details on the primary window's right side.

Running Partition Manager

You can access Partition Manager using any one of the following methods.

- Run Partition Manager directly from the HP-UX command line by issuing this command: `/opt/parmgr/bin/parmgr`

  Command-line options are listed in the *parmgr* (1M) manpage.

- Run SAM (`/usr/sbin/sam`) in graphical mode and select **Partition Manager** to launch Partition Manager.

- Access Partition Manager through a PC Web browser.

  Web access requires that an Apache Web server be installed, configured, and activated on the nPartition where you will run Partition Manager. See the online help's **Starting and Exiting** section for Web configuration details.

When running Partition Manager directly or when launching it from SAM, you must set and export the nPartition system's DISPLAY environment variable. The DISPLAY variable specifies where (which X server) the system displays X windows. You also must use the `xhost` command on the X server to grant access for the nPartition system to display windows on the X server.

See the example below and the *X* (1) and *xhost* (1) manpages for details.

nPartition System

```
# hostname
feshd5a
# export DISPLAY=razmataz:0
# printenv DISPLAY
razmataz:0
#
```

X Server

```
$ hostname
razmataz
$ xhost + feshd5a
feshd5a being added to access control list
$
```

S689

Requirements and Limits

The following are requirements and limits of Partition Manager.

See the *parmgr* (1M) manpage for other requirements.

- Partition Manager provides graphical interfaces only, and does not provide a terminal (text mode) interface.
- Using Partition Manager requires `root` permission.
- HP-UX must be running in multi-user mode to support Partition Manager.
- You can run only one instance of Partition Manager or SAM (`/usr/sbin/sam`) per user login session. To run multiple instances of Partition Manger, you must login separately to launch each.

  Both Partition Manager and SAM use the same lock file (/var/sam/lock/lock_console) to ensure that no more than one instance of either application runs at a time per user login session.
- Partition Manager uses the same driver and library as the HP-UX nPartition commands (the hd_fabric driver and libfab.1 library).
- Partition Manager also provides PCI online card add and replace functionality similar to SAM's, and uses the libolrad.1 library for this functionality.

Partition Manager Online Help

The Partition Manager online help gives complete details on using the Partition Manager utility.

Select the **Help —> Overview** menu item for an online overview.

You also can view Partition Manager help from a Web browser by issuing the following command:

```
/opt/netscape/netscape file:/opt/webadmin/parmgr/help/C/assistance.html
```

Web Site for Partition Manager Information: http://www.software.hp.com/products/PARMGR/info.html

You can find online information about Partition Manager, including manpages, help files, and an interactive demonstration version of Partition Manager, at the `http://www.software.hp.com/products/PARMGR/info.html` Web site.

5688
JP

2 Planning nPartition Configurations

This chapter describes how you can plan nPartition configurations for HP rp7405/rp7410, rp8400, and Superdome servers. Details include the configuration requirements for nPartitions and HP recommendations.

For related procedures to manage nPartitions, refer to the chapter *Managing nPartitions* on page 243.

Also, for an introduction to nPartition features, refer to the chapter *nPartition System Overviews* on page 31.

S687

nPartition Requirements and Recommendations

The hardware *requirements* shown below determine which cells are eligible to be assigned to an nPartition.

Also consider the nPartition *recommendations*, which can improve an nPartition's performance and availability.

Configuration Requirements for nPartitions

Every nPartition you configure must meet the following hardware requirements.

- ☐ All cells in an nPartition **must** have the same *processor revision level and clock speed*. That is, the IODC_HVERSION must be identical for all processors.
- ☐ The same firmware revision **must** be present on all cells within an nPartition.
- ☐ At least one cell in every nPartition **must** be connected to an I/O chassis that has core I/O.

  Only one core I/O is active per nPartition. If an nPartition has multiple cells that are connected to I/O chassis with core I/O, only the core I/O connected to the *active core cell* is active.

Configuration Recommendations for nPartitions

You also should, as possible, configure nPartitions to meet the following configurations for better performance and availability.

- ☐ Each nPartition's size **should** be a power of two: 1, 2, 4, 8, or 16 cells.

  This provides the best memory interleaving and performance characteristics.

  You can configure nPartitions of any size, but those whose size is a power of two have best memory performance.
- ☐ The I/O chassis containing the active core I/O also **should** have an HP-UX boot disk and method of installing or recovering HP-UX (such as a CD-ROM/DVD-ROM drive, network connection to an install server, or tape drive).

5686
21

This allows the nPartition to boot or recover HP-UX, even if only the nPartition's core cell is functioning.

❑ You **should** assign multiple core-capable cells to each nPartition.

This allows the nPartition to boot at least to the BCH interface if a core cell fails to boot.

(Disregard this recommendation if you are configuring multiple nPartitions in an HP rp8400 server or HP rp7405/rp7410 server, each of which has a maximum of two core cells.)

❑ The memory configuration of all cells in an nPartition **should** be identical to achieve best performance.

Each of an nPartition's cells should have:

— the same *number of DIMMs*

— the same *capacity (size)* and the same *locations (population)* of DIMMs

This avoids cell interconnect (crossbar) "hot spots" by distributing memory evenly across all of the nPartition's cells.

❑ The memory configuration of each cell **should** include a multiple of two memory ranks per cell.

Each memory rank is 4 DIMMs. If possible, install memory in sets of 8 DIMMs: 8 DIMMs or 16 DIMMs on HP rp7405/rp7410, HP rp8400, and HP Superdome cells. On HP Superdome cells, you also can install 24 DIMMs or 32 DIMMs per cell.

This provides a performance improvement by doubling the cell's memory bandwidth, as compared to having one memory rank installed.

This also can provide an availability improvement, in that if one memory rank fails the cell still has at least one functional rank of memory.

(At this time memory rank 0 must be functional for a cell to boot.)

❑ Each nPartition **should** have PRI (primary), HAA (high-availability alternate), and ALT (alternate) boot paths defined and configured, and their path flags appropriately configured for your purposes.

5685

The PRI and HAA paths should be configured to reference disks that are connected to different cells, if possible, with HAA being a mirror of the root volume and PRI being the root volume. ALT should be the path of a recovery or install device.

Under this configuration, if the cell to which the PRI disk is connected fails or is otherwise inactive and the HAA disk's cell is available, the nPartition still can boot HP-UX.

Even if the PRI and HAA devices connect to the same cell (such as on a multiple-partition HP rp8400 server), the HAA device can be used to boot the nPartition to HP-UX should the PRI device fail.

5684
21

Configuration Process: Selecting Cells for an nPartition

The following steps provide a basic procedure for selecting which cells to assign to the nPartitions you will create in an HP server.

Selecting Cells for an nPartition

Step 1. Determine the sizes of all nPartitions you will create in the server complex.

Before creating any nPartitions, determine how many nPartitions you plan to configure and establish each nPartition's size (the number of cells).

Step 2. Select the largest undefined nPartition.

If you will configure multiple nPartitions in the complex, assign cells to the largest nPartition first and then configure next largest, and so on, and configure the smallest nPartition last.

Step 3. Choose which cells you will assign to the nPartition by using the nPartition configuration chart for the server model on which you are configuring the nPartitions.

These charts list which cell slots HP supports for assigning to nPartitions, based on the nPartition size and server model.

For nPartition sizes for which HP recommends multiple configurations, select the first available set of cells. For example, for a two-cell nPartition select configuration 2A, if possible, before selecting 2B or 2C.

Step 4. Confirm that the cells you have selected are eligible to be assigned to the nPartition.

For the cells to be eligible, they must meet these requirements:

- The cells **must** not be assigned to another nPartition.
- The cells **must** meet the nPartition hardware requirements (the required processor, firmware, and memory configurations).

S683
21

- The cells **should** be present (installed) in the server and powered on. You can assign cells that are not present or on when using `parcreate` or `parmodify`. However, you should install and power on cells *before* assigning them to nPartitions in order to allow commands to automatically check the cells' compatibility with any other cells in the nPartition. Also note that assigning a cell that is not present or on will cause the nPartition to wait 10 minutes for the cell during the nPartition boot process, if the cell has a "y" use-on-next-boot setting.

If any of the cells does not adhere to these requirements, go back to *Step 3* and select a different set of cells for the nPartition.

Step 5. Assign the cells to the nPartition.

You can either create a new nPartition that includes the selected cells, or you can modify an existing nPartition so that it conforms to the nPartition configuration recommended by the configuration chart.

For specific procedures for assigning cells, refer to the chapter *Managing nPartitions* on page 243.

Step 6. If you still have additional nPartitions for which to select and assign cells, continue with *Step 2*.

Select the largest remaining undefined nPartition, and go back to *Step 2* to choose and assign cells for it.

HP Superdome nPartition Configuration Guidelines

On HP Superdome servers, the locations of the cells you assign to each nPartition and the resulting loads on server interconnections can affect system performance within the server's nPartitions.

HP offers specific guidelines for configuring nPartitions on HP Superdome servers in order to ensure good system performance.

NOTE The guidelines in this section apply to HP Superdome servers only.

These guidelines follow two basic configuration principles:

1. Avoid sharing interconnecting hardware (crossbars and crossbar links) among multiple nPartitions.
2. *Minimize* the number of crossbar links used by each nPartition, *but do not overload* crossbar links by creating nPartitions that can generate more cell communications traffic across the links than the links can support. Overloading crossbar links degrades performance.

The above principles are incorporated into the guidelines below, and are accounted for in the charts of recommended HP Superdome nPartitions.

Also see *nPartition Requirements and Recommendations* on page 110 for other details.

Configuration Guidelines for HP Superdome nPartitions

Use these guidelines to help determine which cells to assign to the nPartitions you create on HP Superdome servers.

❑ **Define nPartitions in order of size.**

Assign cells to the nPartition that has the largest cell count first. Then select cells for the next largest nPartition, and so on, and finally choose cells for the nPartition with the fewest cells last.

5681

This provides more appropriate cell assignments for larger nPartitions (those with more cells). Any smaller nPartitions with fewer cells are more easily accommodated in the remaining, available cells.

❑ **Place each nPartition within an empty cabinet, if possible.**

This applies to nPartitions in HP Superdome 64-way servers only.

If possible, assign each nPartition cells from a cabinet whose cells have no nPartition assignments. Do this before assigning cells from a cabinet that already has cells assigned to an nPartition.

To select cells for nPartitions that are larger than six cells, on HP Superdome 64-way servers, refer *Superdome 64-way Supported nPartition Configurations* on page 121. For such larger nPartitions, assigning some cells from both cabinet 0 and cabinet 1 provides better performance by better distributing cell communications across crossbar links.

These guidelines can help minimize contentions for using the server's interconnecting hardware (crossbars and crossbar links).

❑ **Assign each nPartition cells from an unused "cell quad", if possible.**

Each "cell quad" is a set of four cells that share the same cabinet backplane connections (crossbar chips). Within each HP Superdome cabinet, cell slots 0–3 comprise one cell quad, and cell slots 4–7 comprise the second cell quad.

Because cells in a quad share the same crossbar chips, they have the best cross-cell memory performance.

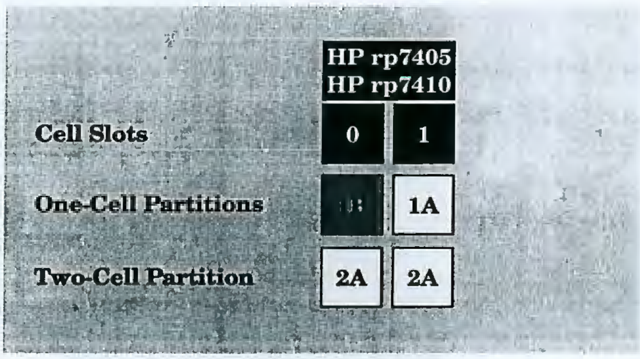
Partitions with cells on different crossbar chips have higher memory latency (worse memory performance) than nPartitions whose cells all share the same crossbar chip.

5680

Chart of Supported HP rp7405/rp7410 nPartition Configurations

Figure 2-1 lists the nPartition configurations that HP supports for HP rp7405/rp7410 servers.

Figure 2-1 **HP rp7405/rp7410 Supported nPartition Configurations**



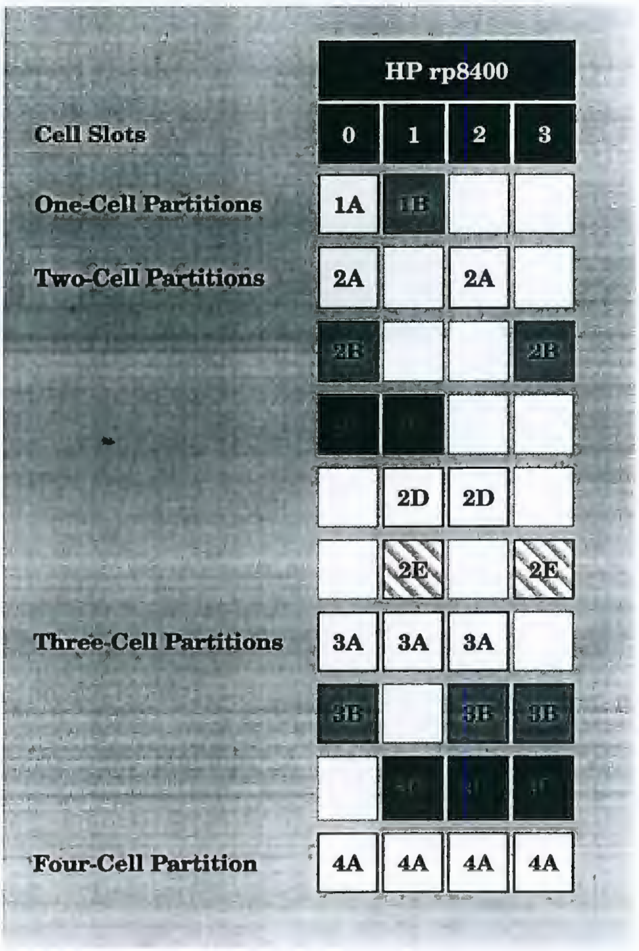
	HP rp7405 HP rp7410	
Cell Slots	0	1
One-Cell Partitions	1B	1A
Two-Cell Partition	2A	2A

8679

Chart of Supported HP rp8400 nPartition Configurations

Figure 2-2 lists the nPartition configurations that HP supports for HP rp8400 servers.

Figure 2-2 **HP rp8400 Supported nPartition Configurations**



	HP rp8400			
Cell Slots	0	1	2	3
One-Cell Partitions	1A	1B		
Two-Cell Partitions	2A		2A	
	2B			2B
	[illegible]	[illegible]		
		2D	2D	
		2E		2E
Three-Cell Partitions	3A	3A	3A	
	3B		3B	3B
		[illegible]	[illegible]	[illegible]
Four-Cell Partition	4A	4A	4A	4A

On HP rp8400 servers, each nPartition must include either cell 0 or cell 1 because these two cells are the server's only core-capable cells.

Charts of Supported HP Superdome nPartition Configurations

Figure 2-3 lists the nPartition cell configurations that HP supports for Superdome 16-way and Superdome 32-way servers.

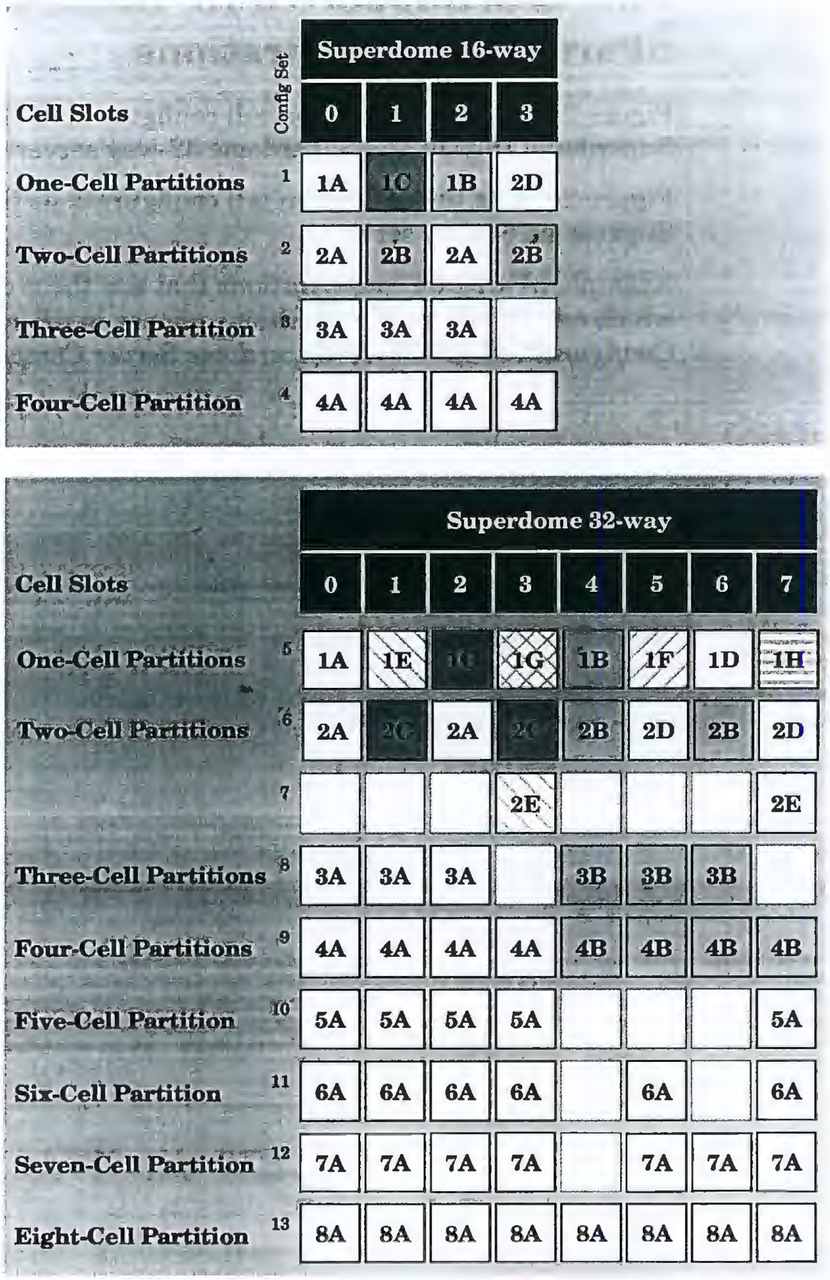
Figure 2-4 lists the nPartition cell configurations that HP supports for Superdome 64-way servers.

Example nPartition configurations that use these charts to determine which cells to assign to nPartitions appear in *nPartition Example Configurations for an HP Superdome Server Complex* on page 122.

5677

Figure 2-3

Superdome 16-way and Superdome 32-way Supported nPartition Configurations



	Config Set	Superdome 16-way			
Cell Slots		0	1	2	3
One-Cell Partitions	1	1A	1C	1B	2D
Two-Cell Partitions	2	2A	2B	2A	2B
Three-Cell Partition	3	3A	3A	3A	
Four-Cell Partition	4	4A	4A	4A	4A

		Superdome 32-way							
Cell Slots		0	1	2	3	4	5	6	7
One-Cell Partitions	5	1A	1E	1C	1G	1B	1F	1D	1H
Two-Cell Partitions	6	2A	2C	2A	2C	2B	2D	2B	2D
	7				2E				2E
Three-Cell Partitions	8	3A	3A	3A		3B	3B	3B	
Four-Cell Partitions	9	4A	4A	4A	4A	4B	4B	4B	4B
Five-Cell Partition	10	5A	5A	5A	5A				5A
Six-Cell Partition	11	6A	6A	6A	6A		6A		6A
Seven-Cell Partition	12	7A	7A	7A	7A		7A	7A	7A
Eight-Cell Partition	13	8A	8A	8A	8A	8A	8A	8A	8A

5676
21

Figure 2-4 **Superdome 64-way Supported nPartition Configurations**

		Superdome 64-way Cabinet 0								Superdome 64-way Cabinet 1							
Cell Slots	Config Set	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
One-Cell Partitions	14	1A	1I	1E	1M	1C	1K	1G	1O	1B	1J	1F	1N	1D	1L	1H	1P
Two-Cell Partitions	15	2A	2E	2A	2E	2C	2G	2C	2G	2B	2F	2B	2F	2D	2H	2D	2H
	16														2I	2I	
	17					2J										2J	
	18				2K				2K				2L				2L
Three-Cell Partitions	19	3A	3A	3A		3C	3C	3C		3B	3B	3B		3D	3D	3D	
	20														3E	3E	3E
Four-Cell Partitions	21	4A	4A	4A	4A	4C	4C	4C	4C	4B	4B	4B	4B	4D	4D	4D	4D
	22					4E		4E							4E		4E
Five-Cell Partitions	23	5A	5A	5A	5A				5A	5B	5B	5B	5B				5B
Six-Cell Partitions	24	6A	6A	6A	6A		6A		6A	6B	6B	6B	6B		6B		6B
Seven-Cell Partitions	25	7A	7A	7A	7A		7A	7B	7A	7B	7B	7B	7B		7B	7A	7B
Eight-Cell Partitions	26	8A	8A	8A	8A	8B	8A	8B	8A	8B	8B	8B	8B	8A	8B	8A	8B
Nine-Cell Partition	27	9A	9A	9A	9A	9A	9A		9A					9A		9A	
Ten-Cell Partition	28	10A	10A	10A	10A	10A	10A	10A	10A					10A		10A	
Eleven-Cell Partition	29	11A	11A	11A	11A	11A	11A	11A	11A					11A	11A	11A	
Twelve-Cell Partition	30	12A	12A	12A	12A	12A	12A	12A	12A					12A	12A	12A	12A
Thirteen-Cell Partition	31	13A	13A	13A	13A	13A	13A	13A	13A				13A	13A	13A	13A	13A
Fourteen-Cell Partition	32	14A	14A	14A	14A	14A	14A	14A	14A		14A		14A	14A	14A	14A	14A
Fifteen-Cell Partition	33	15A	15A	15A	15A	15A	15A	15A	15A		15A	15A	15A	15A	15A	15A	15A
Sixteen-Cell Partition	34	16A	16A	16A	16A	16A	16A	16A	16A	16A	16A	16A	16A	16A	16A	16A	16A

AES—10a-2-PTN

5675

nPartition Example Configurations for an HP Superdome Server Complex

This section shows example cell assignments to demonstrate the procedure for selecting cells for two sample server complex configurations.

For reference in the following examples, Figure 2-3 on page 120 and Figure 2-4 on page 121 list a unique number for each nPartition *configuration set*. (For example, config set 6 shows the four two-cell nPartition configurations that HP recommends for Superdome 32-way servers.)

The following two examples are given here:

- *Example nPartition Configuration for a Superdome 32-way Server* on page 123
- *Example nPartition Configuration for a Superdome 64-way Server* on page 124

S674
21

Example 2-1 Example nPartition Configuration for a Superdome 32-way Server

This example configures an HP Superdome 32-way server with one six-cell nPartition and one two-cell nPartition.

A Superdome 32-way server with a six-cell and two-cell nPartition would be configured with nPartitions 6A and 2B, as shown in Figure 2-3 on page 120.

In Figure 2-3, configuration sets 5–13 are eligible to be assigned on Superdome 32-way servers. The nPartition cell assignments are:

1. 6A (config set 11), the recommended six-cell nPartition.
2. 2B (config set 6), because cells 0 and 2 (2A) are assigned to 6A.
3. nPartitions 6A and 2B use all cells in the complex.

Example
Superdome 32-way complex nPartition configuration:
one six-cell nPartition and one two-cell nPartition.

1	6A	6A	6A	6A		6A		6A
					2B		2B	
2	6A	6A	6A	6A		6A		6A
3	6A	6A	6A	6A	2B	6A	2B	6A

S673
21

Example 2-2

Example nPartition Configuration for a Superdome 64-way Server

This example configures an HP Superdome 64-way server with one seven-cell nPartition and two four-cell nPartitions.

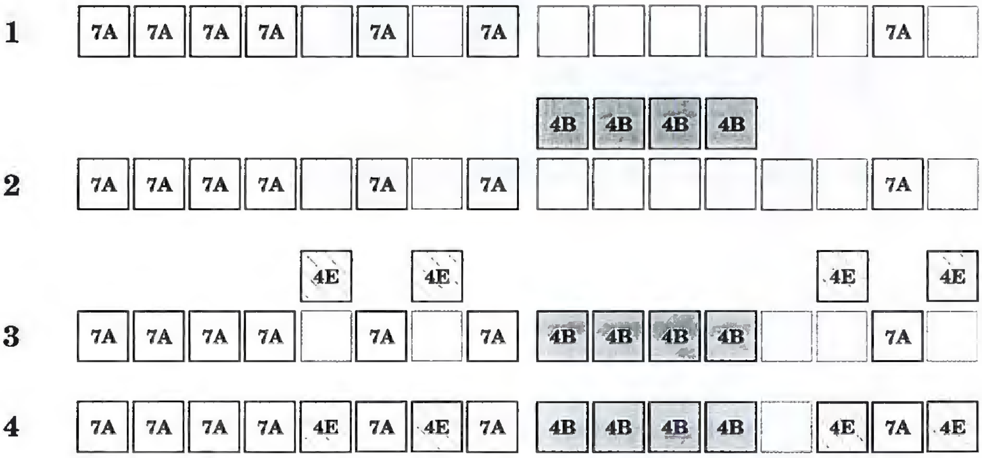
A Superdome 64-way server with a seven-cell nPartition and two four-cell nPartitions would be configured with nPartitions 7A, 4B, and 4E, as shown in Figure 2-4 on page 121.

In Figure 2-4, configuration sets 14–34 are eligible to be assigned on Superdome 64-way servers. The nPartition cell assignments are:

1. 7A (config set 25), the first recommended seven-cell nPartition.
2. 4B (config set 21), because cells in 4A are used by 7A.
3. 4E (config set 22), because some or all cells in 4A–D are assigned.
4. Partitions 7A, 4B, and 4E use all cells except one (cabinet 1, cell 4).

The following illustrations shows how the Superdome 64-way nPartition configurations would be selected, using Figure 2-4 to determine which recommended nPartitions to use.

Example
Superdome 64-way complex nPartition configuration:
one seven-cell nPartition and two four-cell nPartitions.



1	7A	7A	7A	7A		7A		7A							7A	
									4B	4B	4B	4B				
2	7A	7A	7A	7A		7A		7A							7A	
					4E		4E							4E		4E
3	7A	7A	7A	7A		7A		7A	4B	4B	4B	4B			7A	
4	7A	7A	7A	7A	4E	7A	4E	7A	4B	4B	4B	4B		4E	7A	4E

3 Using Console and Service Processor Interfaces

5672

This chapter covers the service processors and nPartition console interfaces available for HP's nPartition servers.

NOTE

The **service processor** in HP servers is sometimes called the Management Processor (MP) and sometimes the Guardian Service Processor (GSP).

Regardless of the name, the service processor in these servers provides approximately the same features and performs essentially the same role.

Throughout this document, the term "service processor" refers to both the MP and GSP service processors.

Service Processor (GSP or MP) Introduction

The **service processor** (GSP or MP) utility hardware is an independent support system for nPartition servers. It provides a way for you to connect to a server complex and perform administration or monitoring tasks for the server hardware and its nPartitions.

The main features of the service processor include the Command menu, nPartition consoles, console logs, chassis code viewers, and nPartition Virtual Front Panels (live displays of nPartition and cell states).

For details, see *Service Processor Features* on page 128.

The service processor is available when its cabinet has standby power, even if the main (48-volt) cabinet power switch is turned off.

Access to the service processor is restricted by user accounts. Each user account is password protected and provides a specific level of access to the server complex and service processor commands.

Multiple users can independently interact with the service processor because each service processor login session is private. However, some output is mirrored: the Command menu and each nPartition console permit one interactive user at a time and mirror output to all users accessing those features. Likewise, the service processor mirrors live chassis codes to all users accessing the Live Chassis Logs feature.

Up to 16 users can simultaneously login to the service processor through its network (customer LAN) interface and they can independently manage nPartitions or view the server complex hardware states.

Two additional service processor login sessions can be supported by the local and remote serial ports. These allow for serial port terminal access (through the local RS-232 port) and external modem access (through the remote RS-232 port).

In general, the service processor (GSP or MP) on nPartition servers is similar to the service processor on other HP servers, while providing enhanced features necessary for managing a multiple-nPartition server.

For example, the service processor manages the complex profile, which defines nPartition configurations as well as complex-wide settings for the server.

S670

The service processor also controls power, reset, and TOC capabilities, displays and records system events (chassis codes), and can display detailed information about the various internal subsystems.

5669
2l

Service Processor Features

The following list describes the primary features available through the service processor (GSP or MP) on HP rp7405/rp7410, HP rp8400, and HP Superdome servers.

- **Command Menu**

  The Command menu provides commands for system service, status, access configuration, and manufacturing tasks.

  To enter the Command menu, enter `CM` at the service processor Main menu. To exit the service processor Command menu, enter `MA` to return to the service processor Main menu.

  See *Using Service Processor Commands* on page 140 for details.

  Service processor commands are restricted based on the three levels of access: Administrator, Operator, and Single Partition User. See *Service Processor Accounts and Access Levels* on page 131 for details.

- **Consoles**

  Each nPartition in a server complex has its own console.

  Enter `CO` at the service processor Main menu to access the nPartition consoles. To exit the console, type **^b** (**Control-b**).

  See *Console Access to nPartitions* on page 150 for details.

  Each nPartition's console output is reflected to all users currently accessing the console.

  One console user can have interactive access to each nPartition's console, and all other users of the console have read-only access. To gain write access for a console, type **^e cf** (**Control-e c f**).

  Each nPartition's console provides access to:

  — Boot Console Handler (BCH) interface for the nPartition.

    The BCH interface is available if the nPartition has booted but has not yet loaded or booted the HP-UX operating system.

  — HP-UX console for the nPartition.

The nPartition console provides console login access to HP-UX and serves as /dev/console for the nPartition.

- **Console Logs**

  Enter **CL** from the service processor Main menu to access the console logs menu. To exit the console log, type ^b (**Control-b**).

  Each nPartition has its own console log, which has a history of the nPartition console's output, including boot output, BCH activity, and any HP-UX console login activity.

  See *Console Log Viewing* on page 155 for details.

  The console log provides a limited history; it is a circular log file that overwrites the oldest information with the most recent.

  All console activity is recorded in the console's log, regardless of whether any service processor users are connected to the console.

- **Error Logs, Activity Logs, and Live Chassis Codes**

  Enter **SL** to access the chassis log viewer. To exit the chassis viewer type ^b (**Control-b**).

  Three types of chassis code log views are available: activity logs, error logs, and live chassis code logs.

  See *Chassis Code Log Viewing* on page 156 for details.

  The activity log and error log provide views of past chassis codes.

  The *live chassis code* view provides:

  — Real-time view of chassis codes.

  — Options for filtering the live chassis code output to show only the chassis codes related to a specific cell (**C**), a specific nPartition (**P**), or alerts (**A**, for codes of alert level 3 and higher). Type **U** to view unfiltered codes (all chassis codes).

  All logs (activity, error, and live) can be displayed in different formats, including: keyword format, text format, hex (with keywords), and raw hex format.

  When viewing chassis logs, type **V** followed by a format selector to change the display format.

- **Virtual Front Panel (VFP) for an nPartition**

  Each nPartition's Virtual Front Panel (VFP) displays real-time status of the nPartition boot status and activity, and details about all cells assigned to the nPartition. The VFP display automatically updates as cell and nPartition status changes. A system-wide VFP also is provided.

  Enter `VFP` at the Main menu to access the View Front Panel menu. To exit a Virtual Front Panel, type `^b` (**Control-b**).

  See *Using Virtual Front Panels* on page 159 for details.

Service Processor Accounts and Access Levels

To access the service processor interface for a server complex, you must have a user account that enables you to login to the service processor.

Each server complex has its own set of service processor user accounts, which are defined for the server complex and may differ from accounts on other complexes.

Service processor user accounts have a specific login name, password, and access level.

The three user account access levels are:

- **Administrator Account**

  Provides access to all commands, and access to all nPartition consoles and Virtual Front Panels.

  Can manage user accounts (using the Command menu `SO` command) and can reconfigure various service processor settings.

- **Operator Account**

  Provides access to a subset of commands, and access to all nPartition consoles and Virtual Front Panels.

  Can reconfigure the service processor.

- **Single Partition User Account**

  Provides access to a restricted subset of commands, and access to a single nPartition's console and a single nPartition's Virtual Front Panel.

  Can only execute commands that affect the *assigned nPartition*.

  Cannot execute commands that could potentially affect multiple nPartitions or affect the service processor configuration.

Each user account can permit multiple concurrent login sessions (if it is a "multiple use" account), or restrict account access to a single login session (for "single use" accounts).

Accessing Service Processor Interfaces

This section describes how to login to the service processor (GSP or MP) for an nPartition server complex.

You can connect to a server complex's service processor using the following methods:

- Connecting through the **customer LAN port** by using `telnet`, if login access through the customer LAN is enabled for the service processor.

  On HP Superdome servers, the customer LAN hardware is labeled "Customer LAN". On HP rp8400 servers it is "GSP LAN". On HP rp7405/rp7410 servers it is the only LAN port on the core I/O.

  Use `telnet` to open a connection with the service processor, then login by entering the account name and corresponding password.

- Connecting through the **local RS-232 port** using a direct serial cable connection.

  On HP Superdome server hardware, the local RS-232 port is labeled "Local RS-232". On HP rp8400 servers it is the "Local Console" port. On HP rp7405/rp7410 servers it is the 9-pin D-shaped connector (DB9) labeled "Console".

- Connecting through the **remote RS-232 port** using external model (dial-up) access, if remote modem access is configured.

  On HP Superdome server hardware, the remote RS-232 port is labeled "Remote RS-232". On HP rp8400 servers it is the "Remote Console" port. On HP rp7405/rp7410 servers it is the DB9 connector labeled "Remote".

S664

Example 3-1 Service Processor Login Session

The following output shows a sample login session for a server whose service processor's hostname is "hpsys-s".

```
> telnet hpsys-s
Trying...
Connected to hpsys-s.rsn.hp.com.
Escape character is '^]'.
Local flow control off

MP login: Accountname
MP password:


                           Welcome to the

                           S Class 16K-A

                        Management Processor

(c) Copyright 1995-2001 Hewlett Packard Co., All Rights
Reserved.

                           Version 0.23



    MP MAIN MENU:

         CO: Consoles
        VFP: Virtual Front Panel
         CM: Command Menu
         CL: Console Logs
         SL: Show chassis Logs
         HE: Help
          X: Exit Connection

MP>
```

S663
2X

Logging in to a Service Processor

This procedure connects to and logs in to a server complex's service processor (GSP or MP) using `telnet` to access the customer LAN.

If connecting through the local or remote RS-232 port, skip *Step 1* (instead establish a direct-cable or dial-up connection) and begin with *Step 2*.

Step 1. Use the HP-UX `telnet` command on a remote system to connect to the service processor for the server complex.

You can connect directly from the command line, for example:

```
telnet sdome-g
```

or run `telnet` first, and then issue the `open` command (for example, `open sdome-g`) at the `telnet>` prompt.

All `telnet` commands and escape options are supported while you are connected to the service processor. See the *telnet*(1) manpage for details.

(On non-HP-UX platforms such as various PC environments you can instead use an alternate `telnet` program.)

Step 2. Login using your service processor user account name and password.

```
GSP login: Accountname
GSP password: Password
```

Step 3. Use the service processor menus and commands as needed and log out when done.

To log out, select the Exit Connection menu item from the Main menu (enter **X** at the `GSP>` prompt or `MP>` prompt).

You also can terminate a login session by issuing the `telnet` escape key sequence **^]** (type: **Control-right bracket**) and entering **`close`** at the `telnet>` prompt.

NOTE If possible, you should log out of any consoles and menus before terminating your telnet session.

5662

If accessing HP-UX on an nPartition, *log out of HP-UX* before exiting the console and service processor sessions. (Otherwise an open HP-UX login session will remain available to any other service processor users.)

S68
3

Using Service Processor Menus

The service processor (GSP or MP) has a set of menus that give you access to various commands, consoles, log files, and other features.

See *Navigating through Service Processor Menus* on page 138 for details on using these menus.

The following menus are available from the service processor Main menu (which is the menu you first access when logging in):

- **Console Menu**—Provides access to consoles for the server's nPartitions.
- **Virtual Front Panel Menu**—Provides a Virtual Front Panel for each nPartition (or for the entire server complex).
- **Command Menu**—Includes service, status, system access, and manufacturing commands.
- **Console Log Viewer Menu**—Allows access to the server's console logs.
- **Chassis Log Viewer Menu**—Allows access to the server's chassis code logs.
- **Help Menu**—Provides online help on a variety of service processor topics and on all service processor Command menu commands.

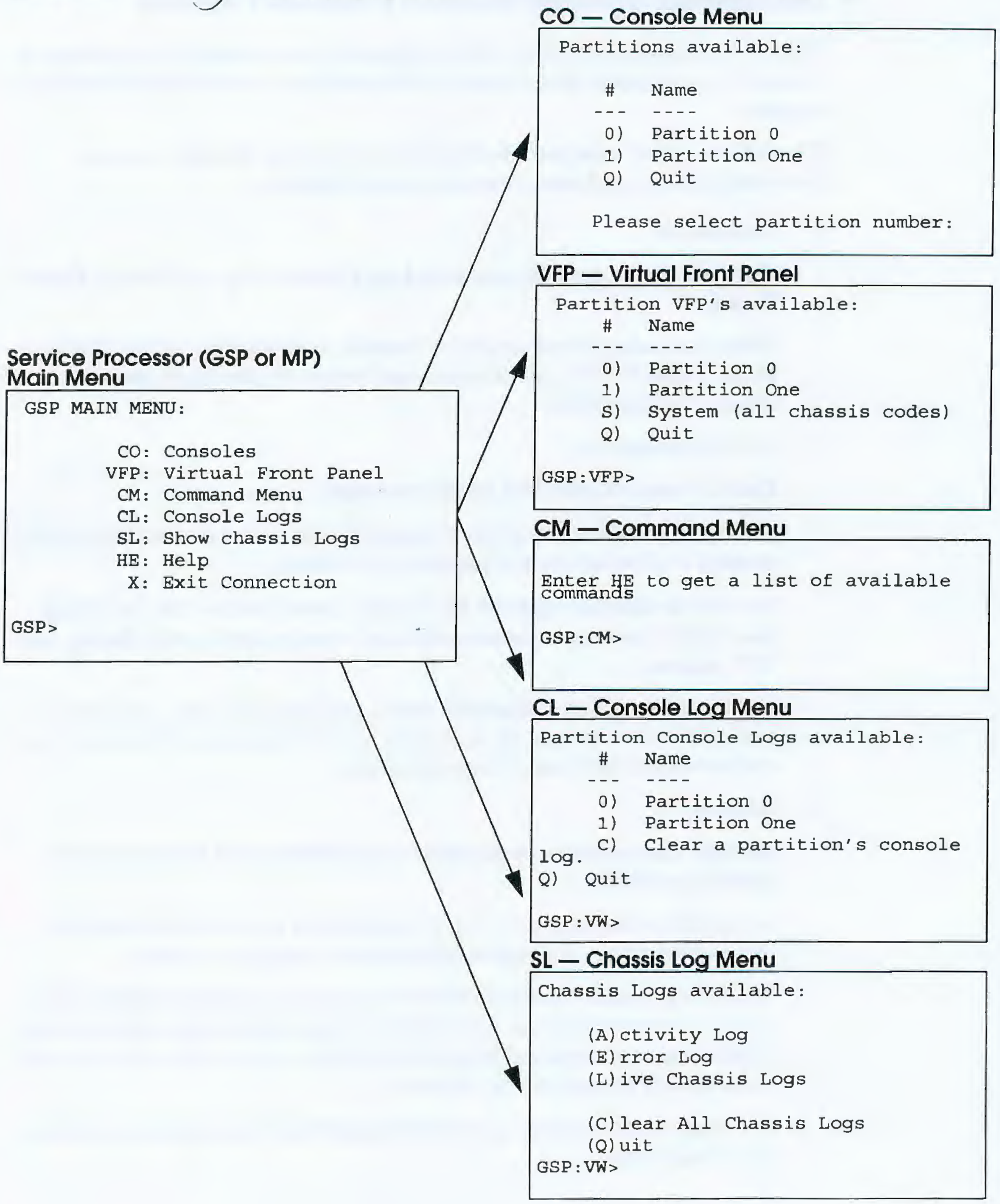
These menus provide a central point for managing an nPartition server complex outside of HP-UX.

The service processor menus provide many tools and details not available elsewhere. More administration features also are available from the nPartition BCH interfaces, or from HP-UX commands and utilities running on one of the server complex's nPartitions.

NOTE

Some specific service processor menu options and features differ slightly on different hardware platforms and firmware revisions. However, most features are identical and behave as described here.

Figure 3-1 Overview of Service Processor (GSP or MP) Menus



Service Processor (GSP or MP) Main Menu

```
 GSP MAIN MENU:

         CO: Consoles
        VFP: Virtual Front Panel
         CM: Command Menu
         CL: Console Logs
         SL: Show chassis Logs
         HE: Help
          X: Exit Connection

GSP>
```

CO — Console Menu

```
 Partitions available:

     #   Name
    ---  ----
     0)  Partition 0
     1)  Partition One
     Q)  Quit

    Please select partition number:
```

VFP — Virtual Front Panel

```
 Partition VFP's available:
      #   Name
     ---  ----
      0)  Partition 0
      1)  Partition One
      S)  System (all chassis codes)
      Q)  Quit

GSP:VFP>
```

CM — Command Menu

```
Enter HE to get a list of available
commands

GSP:CM>
```

CL — Console Log Menu

```
Partition Console Logs available:
      #   Name
     ---  ----
      0)  Partition 0
      1)  Partition One
      C)  Clear a partition's console
log.
Q)  Quit

GSP:VW>
```

SL — Chassis Log Menu

```
Chassis Logs available:

    (A)ctivity Log
    (E)rror Log
    (L)ive Chassis Logs

    (C)lear All Chassis Logs
    (Q)uit
GSP:VW>
```

Navigating through Service Processor Menus

Figure 3-2 on page 139 shows the commands and options for returning to the service processor Main menu and for ending a service processor login session.

The following list also includes tips for navigating through service processor menus and using various menu features:

- `Control-b`

  Exit current console, console log, chassis log, or Virtual Front Panel.

  When accessing an nPartition's console, any log files, or any Virtual Front Panel (VFP), you can exit and return to the Main menu by typing `^b` (**Control-b**).

- `Q` (or lower-case `q`)

  Exit or cancel current menu prompt.

  Enter `Q` (or lower-case q) as response to any menu prompt to exit the prompt and return to the previous sub-menu.

  You can do this throughout the service processor menus, including the console menus, various command menu prompts, and the log and VFP menus.

  Note that, from the Command menu prompt (`GSP:CM>` or `MP:CM>`) you must enter **`MA`** (not Q) to return to the Main menu. However, you can enter `Q` or `q` to cancel any command.

- **Control-]**

  Escape the service processor connection and return to the telnet prompt.

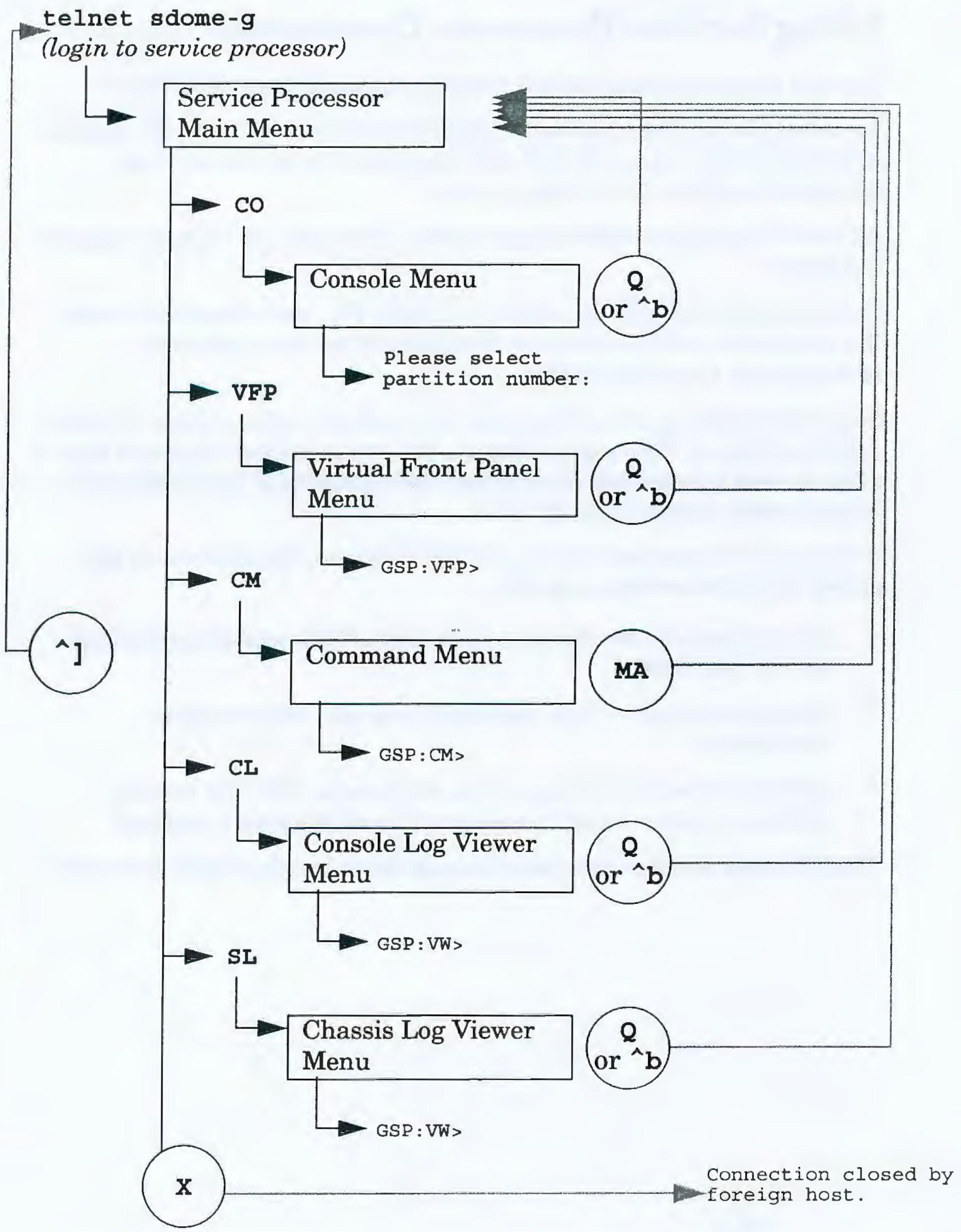
  At any time during your `telnet` connection to a service processor, you can type the `^]` (**Control-right bracket**) escape sequence.

  This key sequence escapes back to the `telnet` prompt. When at the `telnet>` prompt you can use the following commands, among others: **`?`** (print telnet command help information), **`close`** (close the current connection), and **`quit`** (exit telnet).

  To return to the service processor connection, type enter (or return) one or more times.

S658
21

Figure 3-2 Navigating through Service Processor (GSP or MP) Menus



S657

Using Service Processor Commands

You can issue commands at the service processor Command menu.

To access the service processor Command menu, enter **CM** at the service processor's Main menu. To exit the Command menu, enter the **MA** command to return to the Main menu.

All service processor users accessing the Command menu share access to the menu.

Only one command can be issued at a time. For each command issued, the command and its output are displayed to all users currently accessing the Command menu.

Some commands are restricted and are available only to users who have Administrator or Operator privileges. You can issue any command that is valid at your access level by entering the command at the Command menu prompt (`GSP:CM>` or `MP:CM>`).

When you list commands using the **HE** command, the commands are shown in the following categories:

- Service commands—Support boot, reset, TOC, and other common service activities.
- Status commands—Give command help and system status information.
- System and access configuration commands—Provide ways to configure system security and console and diagnostic settings.

The following sections give more details about the available commands.

5656

Commands Commonly Used at the Service Processor

Table 3-1 summarizes commands that are commonly used by system administrators. These commands are available to all service processor users.

Table 3-1 Service Processor: Commonly Used Commands

Command	Description
BO	Boot an nPartition past an inactive boot-is-blocked (BIB) state to make it active.
CP	Display nPartition cell assignments.
HE	Help: list the available commands.
LS	Display LAN connected console status.
MA	Return to the service processor Main menu.
PD	Set the default nPartition for the current session.
PS	Display detailed power and hardware configuration status.
RS	Reset an nPartition.
RR	Reset an nPartition to a *ready for reconfiguration* state, which makes the nPartition inactive.
SYSREV	Display all cabinet FPGA and firmware revisions. (HP rp8400 and HP rp7405/rp7410 only.)
TC	Send a TOC signal to an nPartition.
TE	Broadcast a message to all users of the Command menu.
WHO	List all users connected to the service processor.

The above commonly used commands appear in the service, status, and the system and access configuration categories.

For additional commands, by category, see the following sections.

Service Processor Commands: Quick Reference

The following tables list commands available from the service processor Command menu:

- *Service Commands* on page 142
- *Status Commands* on page 143
- *System and Access Configuration Commands* on page 144

NOTE For a complete and current list of all service processor commands, enter the **HE** command at the service processor Command menu.

Service Commands

The service commands available provide boot, reset, power, TOC, status, and other commands for common service activities.

Table 3-2 Service Processor: Service Commands

Command	Description
BO	Boot an nPartition past an inactive boot-is-blocked (BIB) state to make it active.
DF	Display FRU information of an entity.
MA	Return to the Main menu.
MFG	Enter the manufacturing mode. (Administrator only.)
MR	Modem reset.
PE	Power entities on or off. (Administrator and operator only.)
RE	Reset entity. (Administrator and operator only.)
RR	Reset an nPartition to a *ready for reconfiguration* state, which makes the nPartition inactive.

S6S4

Table 3-2 Service Processor: Service Commands

Command	Description
RS	Reset an nPartition.
SYSREV	Display all cabinet FPGA and firmware revisions. (HP rp8400 and HP rp7405/rp7410 servers only.)
TC	Send a TOC signal to an nPartition.
TE	Broadcast a message to all users of the Command menu.
VM	Margin the voltage in a cabinet. (HP Superdome servers only.)
WHO	Display a list of users connected to the service processor.

Status Commands

The status commands provide command help and system status information, such as hardware status and nPartition configurations.

Table 3-3 Service Processor: Status Commands

Command	Description
CP	Display nPartition cell assignments.
HE	Display the list of available commands.
IO	Display I/O chassis connections to cells. (HP Superdome servers only.)
LS	Display LAN connected console status.
MS	Display the status of the modem.
PS	Display detailed power and hardware configuration status.

S653

System and Access Configuration Commands

The system and access configuration commands provide ways to configure system security and console and diagnostic settings. These commands also enable you to modify some complex configuration settings. Some of these commands are restricted (users with an “Operator” or “Single Partition User” access level can issue a subset of these commands).

Table 3-4 **Service Processor: System and Access Configuration Commands**

Access Level(s)	Command	Description
Administrator	`AR`	Configure the automatic system restart for an nPartition.
Administrator, Operator	`CA`	Configure asynchronous and modem parameters.
Administrator, Operator	`CC`	Initiate a complex configuration.
Administrator	`DATE`	Set the time and date.
Administrator	`DC`	Reset parameters to default configuration.
Administrator, Operator	`DI`	Disconnect remote or LAN console.
Administrator	`DL`	Disable LAN console access.
Administrator	`EL`	Enable LAN console access.
Administrator, Operator, Single Partition User	`ER`	Configure remote/modem port access options.
Administrator, Operator	`FW`	Firmware update utility. (HP rp8400 and HP rp7405/rp7410 servers only.)
Administrator, Operator, Single Partition User	`ID`	Display and/or change certain Stable Complex Configuration Data fields, which describe the complex identity.
Administrator	`IF`	Display network interface information.

5657

Table 3-4 **Service Processor: System and Access Configuration Commands**

Access Level(s)	Command	Description
Administrator, Operator	`IT`	Modify command interface inactivity time-out.
Administrator	`LC`	Configure LAN connections.
Administrator, Operator, Single Partition User	`LS`	Display LAN connected console status.
Administrator	`ND`	Enable/disable network diagnostics.
Administrator, Operator	`PD`	Set the default nPartition for the current session.
Administrator, Operator	`PWRGRD`	Configure power grid settings. (HP rp8400 and HP rp7405/rp7410 servers only.)
Administrator, Operator	`RL`	Rekey complex profile lock.
Administrator	`SO`	Configure security options and access control.
Administrator, Operator	`XD`	Service processor diagnostics and reset options.

Network Configuration for a Service Processor

This section describes how to list and configure the network settings for service processor (GSP or MP) hardware. These settings are used for connections to the service processor and are not used for HP-UX networking.

Details on configuring service processor networking are given in the procedure *Configuring Service Processor Network Settings* on page 148.

The service processor utility hardware on HP Superdome servers has two network connections: the customer LAN and private LAN. The service processor on HP rp8400 and HP rp7405/rp7410 servers do not have a private LAN but have only customer LAN connections.

Features of service processor LANs are given in the following list.

- **Customer LAN for Service Processor**

  The **customer LAN** is the connection for login access to the service processor menus, consoles, commands, and other features.

  All HP nPartition servers have a customer LAN.

  On HP Superdome servers, the customer LAN port is labeled "Customer LAN". On HP rp8400 servers it is "GSP LAN". On HP rp7405/rp7410 servers it is the only LAN connection on each core I/O board.

- **Private LAN for Service Processor (Superdome Only)**

  The **private LAN** is the connection to the Superdome service support processor (SSP) workstation.

  Only Superdome servers have a private LAN.

To *configure* service processor network settings, you can use the the Command menu's LC command.

To *list* the current service processor network configuration use the LS command.

The following examples show service processor LAN status for various HP nPartition servers.

HP rp7405/rp7410 or rp8400 Service Processor LAN Status

```
MP:CM> LS

Current configuration of MP customer LAN interface
  MAC address    : 00:30:6e:05:19:ac
  IP address     : 15.99.84.140     (0x0f63548c)
  Hostname       : redxii-c
  Subnet mask    : 255.255.255.0    (0xffffff00)
  Gateway        : 15.99.84.254     (0x0f6354fe)
  Status         : UP and RUNNING
  AutoNegotiate  : Enabled
  Data Rate      : 100 Mb/s
  Duplex         : Half
  Error Count    : 0
  Last Error     : none

MP:CM>
```

HP Superdome Service Processor LAN Status

```
GSP:CM> LS

Current configuration of GSP customer LAN interface
  MAC address : 00:10:83:27:04:5a
  IP address  : 15.99.49.129     0x0f633181
  Name        : feshd5-u
  Subnet mask : 255.255.248.0    0xfffff800
  Gateway     : 15.99.49.254     0x0f6331fe
  Status      : UP and RUNNING

Current configuration of GSP private LAN interface
  MAC address : 00:a0:f0:00:83:b1
  IP address  : 192.168.2.15     0xc0a8020f
  Name        : priv-05
  Subnet mask : 255.255.255.0    0xffffff00
  Gateway     : 192.168.2.100    0xc0a80264
  Status      : UP and RUNNING

GSP:CM>
```

Default Service Processor Network Settings

Table 3-5 and Table 3-6 list the default customer LAN and private LAN network settings for nPartition servers. Only Superdome servers have a private LAN.

Table 3-5 Default Configuration for Service Processor Customer LAN (All nPartition Servers)

Customer LAN IP Address	192.168.1.1
Customer LAN Host Name	gsp0
Customer LAN Subnet Mask	255.255.255.0
Customer LAN Gateway	192.168.1.1

SD49

Table 3-6 Default Configuration for Service Processor Private LAN (HP Superdome Servers Only)

Private LAN IP Address	192.168.2.10
Private LAN Host Name	priv-00
Private LAN Subnet Mask	255.255.255.0
Private LAN Gateway	192.168.2.10

Configuring Service Processor Network Settings

This procedure (Command menu, **LC** command) configures the service processor's customer LAN and private LAN network settings from the service processor Command menu.

Step 1. Connect to the server complex's service processor, login as an administrator, and enter **CM** to access the Command menu.

Use `telnet` to connect to the service processor, if possible.

If a service processor is at its default configuration (including default network settings), you can connect to it using either of these methods:

- Establish a direct serial cable connection through the service processor's local RS-232 port, a 9-pin D-shaped connector (DB9).

  On HP Superdome servers this port is labeled "Local RS-232". On HP rp8400 servers it is the "Local Console" port. On HP rp7405/rp7410 servers use the DB9 connector that is labeled "Console".

- Access a PC or workstation on the same subnet as the service processor, modify its network routing tables to include the default customer LAN IP address, then `telnet` to the service processor. The procedure to modify networking and connect is:

  1. Access a PC or workstation on the service processor's subnet.
  2. Modify the network routing tables for the PC or workstation by using the **`route add 192.168.1.1`** ***`ClientName`*** command, where *`ClientName`* is the network name of the PC or workstation.

5648
71

From a PC command prompt: `route add 192.168.1.1 ClientName`
On an HP-UX workstation login as root and use this command:

```
/usr/sbin/route add 192.168.1.1 ClientName
```

After you reconfigure the service processor's networking, you can remove these network routing table changes with the `route delete...` command.

3. Enter this command to confirm the new network connection to the service processor: **`ping 198.168.1.1 -n 2`**

4. Use the **`telnet 192.168.1.1`** command from the PC or workstation to connect to the service processor.

Step 2. From the service processor Command menu, enter **`LS`** to *list* the current network settings, and if needed use the **`LC`** command to *reconfigure* the network settings for the service processor.

You must be logged in as an administrator to use the `LC` command.

The `LC` command enables you to modify the customer LAN and/or the private LAN configuration.

You can cancel all changes to the service processor LAN configuration at any time by replying **`Q`** to any of the `LC` command's prompts.

S647

Console Access to nPartitions

The service processor Console menu provides access to all nPartition consoles within the server complex.

Enter `CO` from the service processor Main menu to access an nPartition's console. To exit the nPartition console, type `^b` (**Control-b**) to return to the Main menu.

Each nPartition in a complex has a single console. However, multiple connections to the console are supported, allowing multiple users to simultaneously view the console output. Only one connection per console permits write-access.

To force (gain) console write access for an nPartition's console, type **`^ecf`** (**Control-e c f**).

Each nPartition console can display a variety of information about the nPartition, including:

- Partition startup, shutdown, and reset output.
- Boot Console Handler (BCH) menus, if the nPartition has not yet booted the HP-UX operating system and has completed Power-On Self Tests (POST).
- The HP-UX login prompt and "console shell access".

nPartition Console Access versus Direct HP-UX Login

You may need to consider the following factors when deciding whether to interact with an nPartition through the service processor console interface or a direct HP-UX login:

- Whether you want to log your activity to the nPartition's console log (all console activity is stored at least temporarily).
- Whether HP-UX is installed, booted, and properly configured on the nPartition.

  If HP-UX is not installed on an nPartition, you should access the nPartition's console (through the service processor) in order to install and configure HP-UX.

5646

You should login to HP-UX running on an nPartition when you do not need to use service processor features and do not want to record a log of your activity.

Before HP-UX has booted, the service processor nPartition consoles are the primary method of interacting with an nPartition.

After an nPartition has booted HP-UX, you should be able to connect to and login to the nPartition by using `telnet` or `rlogin` to remotely login.

If the HP-UX kernel booted on the nPartition does not have networking fully configured, you may need to login using a service processor nPartition console connection to set up the nPartition's networking configuration (using `/sbin/set_parms`).

To view the /dev/console messages for HP-UX running on an nPartition, you can access the nPartition's console, view its console log, or use the `xconsole` command or `xterm -C` command and option. See the *xconsole* (1) or *xterm* (1) manpages for details.

Boot Console Handler (BCH) Access

S645

Each nPartition in a server complex has its own Boot Console Handler (BCH) interface. When an nPartition is booted to BCH, its BCH interface is available through the nPartition's console.

The nPartition BCH interface enables you to manage and configure the HP-UX boot process for an nPartition. You also can configure some settings for the local nPartition, get some information about the nPartition and its server complex, and perform other tasks such as reboot.

Figure 3-3 shows details on accessing and using an nPartition's BCH interface, including the following points:

- To access an nPartition's console type `CO` from the service processor (GSP or MP) Main menu.
- To force console write access, type `^ecf` (**Control-e c f**).
- To exit the console, type `^b` (**Control-b**) to return to the Main menu.

The BCH interface is available after an nPartition's cells have been powered on; its hardware has completed all Power-On Self Tests (POST); and the cells have booted past boot-is-blocked, rendezvoused, and BCH has started executing. Refer to the chapter *An Overview of nPartition Boot and Reset* on page 161 for details.

Once you begin the HP-UX boot process and load ISL, the BCH interface is no longer available.

The BCH menus and commands for nPartitions differ slightly from the commands menus for BCH on other HP 9000 server systems.

To display the *current* BCH menu and commands, type `DI`.

The BCH interface's `HELP` command lists BCH command or menu details.

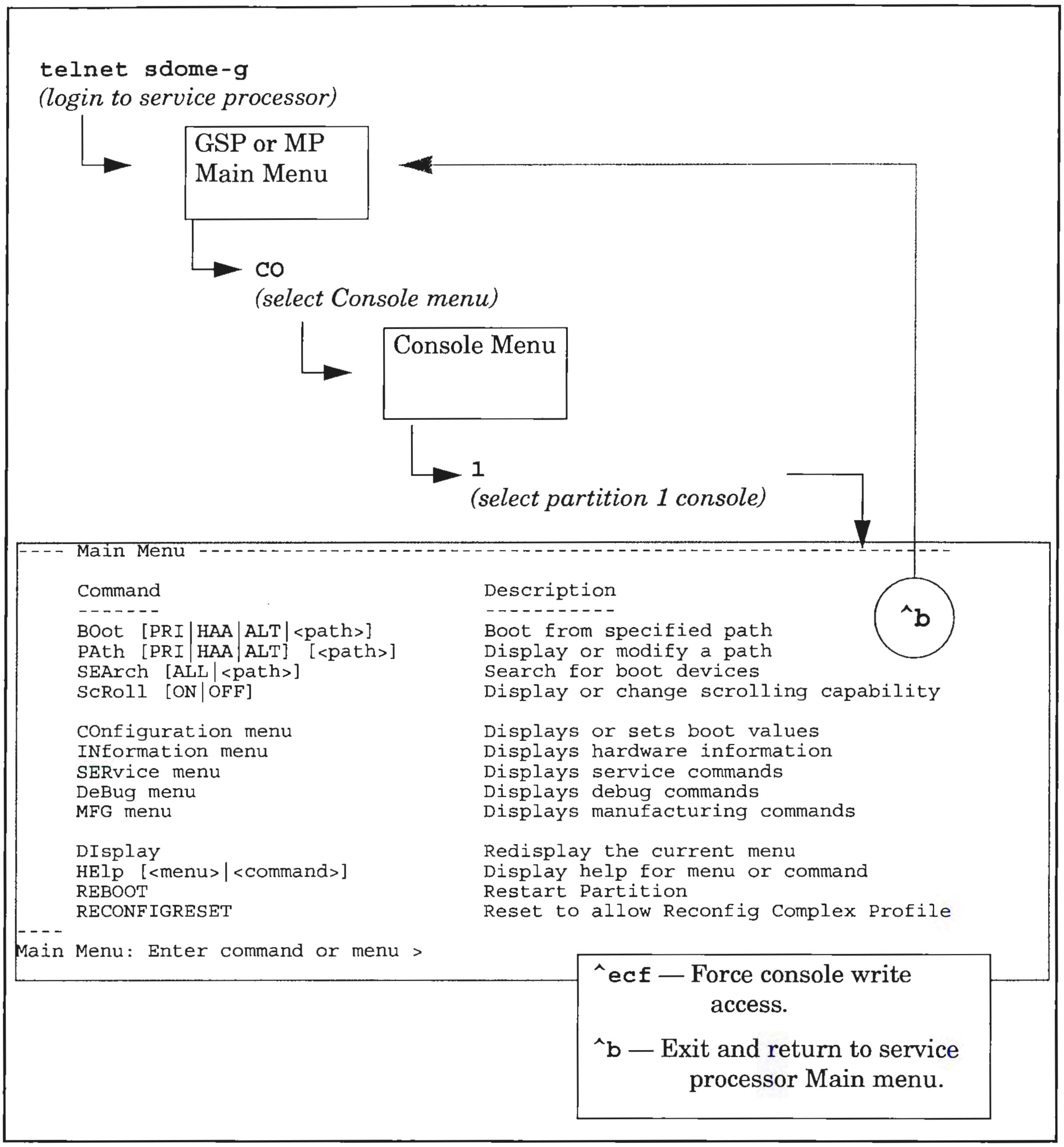
NR

```
Main Menu: Enter command or menu > HELP MA
---- Main Menu Help ----------------------------------------------------------

     The following submenus are available from the main menu:

     COnfiguration------------------------------------BootID
     INformation-----------------------ALL            BootTimer
     SERvice-------------BAttery       BootINfo       CEllConfig
                         CLEARPIM      CAche          COreCell
                         MemRead       ChipRevisions  CPUConfig
                         PDT           ComplexID      DataPrefetch
                         PIM           FabricInfo     DEfault
                         SCSI          FRU            FastBoot
                                       FwrVersion     KGMemory
                                       IO             PathFlag
                                       LanAddress     PD
                                       MEmory         ResTart
                                       PRocessor      TIme
...
```

S644

S643

Figure 3-3 **Accessing an nPartition's BCH Interface**



`telnet sdome-g`
(login to service processor)

GSP or MP Main Menu

`CO`
(select Console menu)

Console Menu

`1`
(select partition 1 console)

```
---- Main Menu ---------------------------------------------------------------

     Command                           Description
     -------                           -----------
     BOot [PRI|HAA|ALT|<path>]         Boot from specified path
     PAth [PRI|HAA|ALT] [<path>]       Display or modify a path
     SEArch [ALL|<path>]               Search for boot devices
     ScRoll [ON|OFF]                   Display or change scrolling capability

     COnfiguration menu                Displays or sets boot values
     INformation menu                  Displays hardware information
     SERvice menu                      Displays service commands
     DeBug menu                        Displays debug commands
     MFG menu                          Displays manufacturing commands

     DIsplay                           Redisplay the current menu
     HElp [<menu>|<command>]           Display help for menu or command
     REBOOT                            Restart Partition
     RECONFIGRESET                     Reset to allow Reconfig Complex Profile
----
Main Menu: Enter command or menu >
```

`^ecf` — Force console write access.

`^b` — Exit and return to service processor Main menu.

5642

Console Log Viewing

Each nPartition in a server complex has its own console log that stores a record of the nPartition's most recent console activity.

To access an nPartition's console log, enter `CL` from the service processor Main menu and select which nPartition's console log you want to view. To exit the console log viewer, type `^b` (**Control-b**) to return to the Main menu.

When viewing an nPartition's console log, type `P` to view the previous page of the console log, or type `N` (or **Enter**) to view the next page.

When you enter an nPartition's console log viewer it displays the oldest data in the log first and allows you to page through the log to view the more recently recorded activity.

Each nPartition's console log is a circular log file that records approximately 30 to 40 pages of data. All nPartition console activity is written to this log file, regardless of whether a user is connected to the nPartition console.

As an nPartition's console log is written the oldest data in the log is overwritten by current data, as needed, so that the last 30 to 40 pages of console output always is available from the console log viewer.

5641

Chassis Code Log Viewing

The service processor's **chassis log viewer** enables you to view chassis codes that are emitted throughout the entire server complex.

To enter the chassis log viewer enter `SL` at the service processor Main menu. To exit the viewer type `^b` (**Control-b**) to return to the Main menu.

Chassis codes are data that communicate information about system events from the source of the event to other parts of the server complex. Chassis code data indicates what event has occurred, when and where it happened, and its severity (the *alert level*).

All chassis codes pass from the event source through the service processor. The service processor takes any appropriate action and then reflects the chassis codes to all running nPartitions. If an nPartition is running event monitoring software, it may also take action based on the chassis codes (for example, sending notification e-mail).

System administrators, of course, may have interest in viewing various chassis codes—especially chassis codes that indicate failures or errors.

Hardware, software, and firmware events may emit chassis codes as a result of a failure or error, a major change in system state, or basic forward progress. For example: a fan failure, an HPMC, the start of a boot process, hardware power on or off, and test completion all result in chassis codes being emitted.

While HP-UX is running on an nPartition, it constantly emits a "heartbeat" chassis code (at alert level 0) to indicate that the operating system still is functioning and has not hung.

NOTE

Each nPartition server cabinet's **front panel attention LED** is automatically *turned on* when one or more chassis codes of *alert level 2* or higher have not yet been viewed by the administrator. When this attention LED is on, entering the chassis log viewer turns the LED off.

You can remotely check this attention LED's on/off status by using the service processor Command menu's `PS` command, `G` option.

S640

On nPartition servers, chassis codes are recorded in the server complex **activity log** (for events of alert level 0 or alert level 1) or the **error log** (for events alert level 2 or higher).

```
GSP> SL

Chassis Logs available:

    (A)ctivity Log
    (E)rror Log
    (L)ive Chassis Logs

    (C)lear All Chassis Logs
    (Q)uit

GSP:VW> L

        Entering Live Log display

        A)lert filter
        C)ell filter
        P)artition filter
        U)nfiltered
        V)iew format selection
        ^B to Quit

Current filter: ALERTS only
```

Log Viewing Options: Activity, Error, and Live Chassis Logs

When you enter the chassis log viewer by entering `SL` at the service processor (GSP or MP) Main menu, you can select from these viewers:

- **Activity Log Viewer**

  Allows you to browse recorded chassis codes of alert level 0 or 1.

- **Error Log Viewer**

  Allows you to browse recorded chassis codes of alert level 2 or higher.

- **Live Chassis Logs Viewer**

  Displays chassis codes in real time as they are emitted.

  By default, the live chassis code viewer has the *Alert filter* enabled, which causes it to display only the events of alert level 3 or higher.

  To view all chassis codes in real-time, type `U` for the *Unfiltered* option.

You also can filter the live codes by cell (`C`) or nPartition (`P`). *Cell filter*: only display chassis codes emitted by a specific cell in the server complex. *Partition filter*: only display chassis codes emitted by hardware assigned to a specific nPartition.

When viewing chassis code logs, type `V` to change the display format. The viewers can show chassis codes in text format (`T`), keyword format (`K`), or raw hex format (`R`).

Using Virtual Front Panels

The Virtual Front Panel (VFP) provides ways to monitor the chassis codes for a particular nPartition or the entire server complex (all nPartitions).

The VFP presents a real-time display of activity on the selected nPartition(s) and it automatically updates when cell and nPartition status change.

To access the VFP feature, enter **VFP** from the service processor Main menu. To exit the VFP, type **^b** (**Control-b**) to return to the Main menu.

When you access a Virtual Front Panel, you can either select the nPartition whose VFP you want to view or select the system VFP to view summary information for all nPartitions in the server complex.

```
E indicates error since last boot
     Partition 0  state            Activity
     ------------------            --------
     Cell(s) Booting:    710 Logs

  #  Cell state                    Activity
  -  ----------                    --------
  0  Early CPU selftest            Cell firmware test                   232  Logs
  1  Early CPU selftest            Processor test                       230  Logs
  2  Memory discovery              Physical memory test                 242  Logs





GSP:VFP (^B to Quit) >
```

When you access a service processor using a single-partition user account, using the VFP feature enables you to view only the VFP for the nPartition to which you have access.

S636

4 An Overview of nPartition Boot and Reset

5635

This chapter presents an overview of booting and reset concepts and issues for HP nPartition servers.

For procedures to boot, reboot, and configure boot options, refer to the chapter *Booting and Resetting nPartitions* on page 197.

NOTE For details on booting and rebooting virtual partitions within an nPartition, refer to the chapter *Virtual Partitions (vPars) Management on nPartitions* on page 441.

Types of Booting and Resetting for nPartitions

All standard boot and reboot methods are supported for HP nPartition servers, though some boot and reset procedures differ slightly or use different tools than on other HP servers.

HP's nPartition servers also provide two special types of reboot and reset for managing nPartitions: performing a **reboot for reconfig**, and resetting an nPartition to the **ready for reconfig** state.

The following list summarizes all types of booting, rebooting, and resetting that are supported for HP nPartition systems. See the *Reboot for Reconfig* and *Ready for Reconfig State* items for a discussion of these nPartition-specific boot processes.

NOTE When rebooting HP-UX on an nPartition under normal circumstances—such as when *not* reconfiguring or halting it—use the `shutdown -r` command.

- **Reboot**

  A **reboot** shuts down HP-UX and reboots the nPartition.

  Only the nPartition's *active* cells are rebooted.

  To perform a standard reboot of an nPartition use the `shutdown -r` command.

- **Halt**

  A **halt** shuts down HP-UX, halts all processing on the nPartition, and does not reboot.

  To perform this task use the `shutdown -h` command.

  To reboot a halted nPartition use the service processor Command menu's `RS` command.

- **Reset**

  A **reset** resets the nPartition immediately. Only the nPartition's *active* cells are reset.

  You can reset an nPartition using the BCH interface's `REBOOT` command or the service processor Command menu's `RS` command.

  The `RS` command *does not check* whether the specified nPartition is in use or running HP-UX—be certain to correctly specify the nPartition.

- **Boot an nPartition from the Service Processor (GSP or MP)**

  A **boot** initiated from the service processor boots an inactive nPartition past the *ready for reconfig* state.

  The nPartition's cells proceed past boot-is-blocked (BIB), rendezvous, and the nPartition boots to the BCH interface.

  To boot an inactive nPartition, use the service processor Command menu's `BO` command.

- **Boot HP-UX from the BCH Interface**

  To **boot** HP-UX on an nPartition, use the BCH interface's `BOOT` command and specify the device path from which the program loaders and HP-UX kernel .

  The BCH interface's `BOOT` command loads and boots HP-UX on an nPartition. This command also can be used to load and interact with the Initial System Loader (ISL) interface. Likewise on Superdome servers the virtual partitions monitor (`MON>` prompt) is loaded following the `BOOT` command.

- **Reboot for Reconfig**

  A **reboot for reconfig** shuts down HP-UX, resets all cells assigned to the nPartition, performs any nPartition reconfigurations, and boots the nPartition back to the BCH interface.

  To perform a reboot for reconfig of the local nPartition, use the `shutdown -R` command.

  All cells—including any inactive cells and all newly added or deleted cells—reboot and are reconfigured. All cells with a "y" *use-on-next-boot* setting participate in partition rendezvous and synchronize to boot as a single nPartition.

S637

After you assign a cell to an nPartition, or remove an active cell from an nPartition, you can perform a reboot for reconfig of the nPartition to complete the cell addition or removal.

If an nPartition is configured to boot HP-UX automatically, it can do so immediately following a reboot for reconfig.

- **Ready for Reconfig State**

  A reboot to the **ready for reconfig** state shuts down HP-UX, resets all cells assigned to the nPartition, performs any nPartition reconfigurations, and keeps all cells at a boot-is-blocked (BIB) state, thus making the nPartition and all of its cells inactive.

  When an nPartition is at the ready for reconfig state you can add or remove cells from the nPartition from a remote nPartition within the server complex.

  To put an nPartition into the ready for reconfig state use the `shutdown -R -H` command, the BCH interface's `RECONFIGRESET` command, or the service processor Command menu's `RR` command.

  To make an nPartition boot past ready for reconfig, use the service processor Command menu's `BO` command. The `BO` command makes the nPartition active by allowing its cells to boot past BIB, rendezvous, and boot to the BCH interface (and, if configured, automatically boot HP-UX).

- **TOC: Transfer-of-Control Reset**

  When you initiate a **transfer-of-control reset**, the service processor immediately performs a TOC reset of the specified nPartition, which resets the nPartition and allows a crash dump to be saved.

  If crash dump is configured for HP-UX on an nPartition, then when you TOC the nPartition while it is running HP-UX, the nPartition performs a crash dump and lets you select the type of dump.

  To perform a TOC reset, use the service processor Command menu's `TC` command.

  HP nPartition systems do not have TOC buttons on the server cabinet hardware.

S631
21

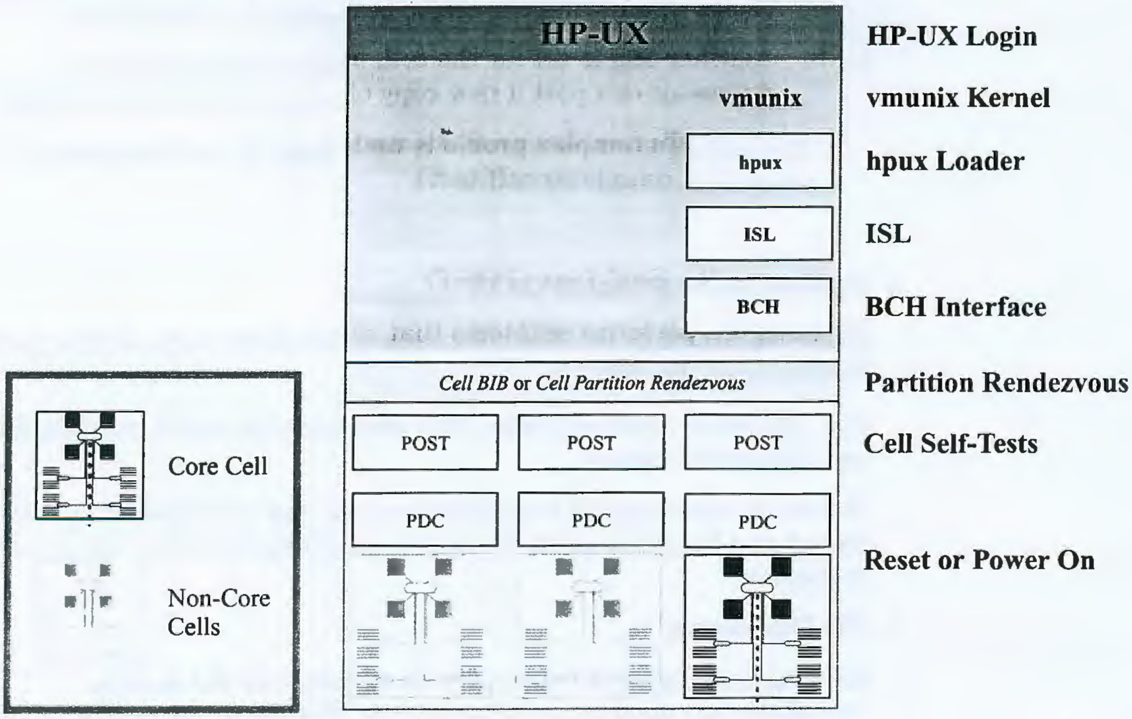
Boot Process for nPartitions, Cells, and HP-UX

The boot process for nPartitions is similar to the process on other HP servers. However, on HP nPartition servers, each cell boots and performs self tests (POST) separately, and one or more cells rendezvous to form an nPartition before providing a BCH interface for the nPartition.

NOTE This section covers nPartitions booting HP-UX in *non-vPars mode*.

For details on virtual partitions (vPars), refer to the chapter *Virtual Partitions (vPars) Management on nPartitions* on page 441.

Figure 4-1 **nPartition HP-UX Boot Process (non-vPars Mode)**



S630

Each nPartition goes through the boot process shown in Figure 4-1, from power on to booting HP-UX:

1. **Power On or Reset**

   The boot process starts when any of the following events occurs:

   - An nPartition is reset or rebooted.
   - The entire server complex is powered on.
   - Power is turned on for components in the nPartition (such as cells).

2. **Processor Dependent Code (PDC)**

   The monarch processor on each cell runs its own copy of the PDC firmware.

   a. The boot-is-blocked (BIB) flag is set for the cell.

      The BIB flag remains set until the service processor (GSP or MP) clears it, allowing the cell to boot as part of an nPartition.

   b. Another flag is set for the cell, indicating that the service processor can post a new copy of the complex profile to the cell.

      The cell's complex profile is updated later in the boot process, after it completes self-tests.

3. **Power-On Self-Test (POST)**

   Each cell performs self-tests that check the processors, memory, and firmware on the cell.

   If a component fails self-tests, it is deconfigured and if possible the cell continues booting.

   Following this step, all components in the cell are known and are tested and the cell reports its hardware configuration to the service processor.

4. **I/O Discovery**

   Each cell performs I/O discovery and configures I/O busses, including: any system bus adapter (the SBA for an I/O card cage) and its local bus adapters (LBAs, one per PCI card slot in the card cage).

5029

Following this, any I/O busses connected to the cell are known and configured by the cell.

5. **Boot-Is-Blocked (BIB) or Partition Rendezvous**

   Each cell either will remain at a boot-is-blocked state (spins at BIB) or will rendezvous with any other available cells in the nPartition.

   Cells that remain at BIB are *inactive*, and cells that rendezvous into the nPartition are *active*.

   - **Boot-Is-Blocked (BIB)**

     A cell remains at boot-is-blocked (and thus is *inactive*) in any of the following cases:

     — The cell has a "n" use-on-next-boot setting.

     — The cell boots too late to participate in nPartition rendezvous.

     — The cell's nPartition has been reset to the ready for reconfig state.

     In this case, all of the nPartition's cells remain at boot-is-blocked.

     — The cell fails self-tests that cause the cell to not be usable in the nPartition.

   - **Partition Rendezvous**

     Partition rendezvous of all cells occurs in the following manner:

     — Partition rendezvous begins when the first of the nPartition's cells has completed self-tests and I/O discovery.

     — The nPartition is allowed up to ten minutes for all cells with a "y" use-on-next-boot setting to participate in partition rendezvous.

       — Once all assigned cells with a "y" use-on-next-boot setting have entered the rendezvous stage, partition rendezvous can complete.

       All cells participating in rendezvous are active cells whose resources (processors, memory, I/O) are used by the nPartition.

5628

- If any cells with a "y" use-on-next-boot setting *do not* report to rendezvous, then ten minutes after rendezvous began the cells that have not reported become inactive cells, and all other reporting cells complete rendezvous and are active.

  The inactive cells' resources are not available to be used by the nPartition, although the cells still are assigned to the nPartition.

6. **Boot Console Handler (BCH)**

   The BCH interface provides the main method for interacting with an nPartition during its boot process.

   BCH runs on top of PDC, and it provides menus for getting nPartition status, for configuring nPartition boot settings, and for booting HP-UX and rebooting the nPartition.

   One processor on the nPartition's core cell runs BCH and all other processors in the nPartition are idle while the BCH interface is available.

   An nPartition can immediately proceed past BCH to boot HP-UX when the nPartition's boot paths are set and boot actions for the paths are configured to automatically boot.

7. **Initial System Loader (ISL) and Secondary System Loader (hpux)**

   In most situations you do not need to use the ISL and hpux interfaces.

   However, when using the BCH interface's BOOT command you can select to stop at the ISL prompt to perform more detailed booting tasks.

   For example, you can use the ISL interface to boot HP-UX in single-user or LVM-maintenance mode, or to boot an HP-UX kernel other than /stand/vmunix.

8. **HP-UX Operating System**

   The HP-UX operating system boots on an nPartition after ISL and the Secondary System Loader (hpux) specify which kernel is to be booted.

   By default, on HP-UX boot disks, the AUTO file specifies that the /stand/vmunix kernel is booted.

5627

For example, when you configure boot paths and boot actions to automatically boot HP-UX, the ISL and hpux loaders specify that the /stand/vmunix kernel is booted.

Overview of nPartition Boot Features

S026

This section lists several boot issues particular to HP nPartition servers.

Each nPartition is booted, rebooted, shut down, and reset individually. In many situations you can boot and reboot nPartitions using the same basic procedures that are used on other HP servers.

The following list describes notable features related to booting, rebooting, and power cycling nPartitions:

- Each nPartition can boot and reboot independently of other nPartitions. Resetting one nPartition has no effect on the others.
- You can perform many reset and power cycling tasks remotely.

  You can reset and control power from an nPartition server's service processor Command menu, from the BCH interface for an nPartition, or from HP-UX running on an nPartition.
- In order to contribute resources to an nPartition, the cells (and I/O chassis) assigned to the nPartition must be powered on and booted in time to participate in partition rendezvous.

  Otherwise, the cells will remain inactive (though still assigned to the nPartition) and their processors, memory, and any I/O will not available for use.
- Three boot path variables—PRI, HAA, and ALT—are supported for each nPartition.

  PRI typically is the primary HP-UX boot device, HAA typically is a mirror of the root volume, and ALT is for install or recovery media such as tape or DVD-ROM devices.
- You can specify a *boot action* for each boot path variable. The boot action determines what action (for example: boot HP-UX) is taken when the nPartition boots and reaches the BCH interface.

  To set boot actions, use the BCH Configuration menu's PathFlags (`PF`) command. The `setboot` command can configure the PRI actions only.

  When an nPartition boots to BCH, it attempts to perform the PRI path's boot action. The HAA path and ALT path boot actions also can be attempted, in that order, depending on the PRI settings.

5625

- *Before powering off* a cell, the cell should be inactive; unassigned; or assigned to an nPartition that either has been shut down and halted or has been reset to the ready for reconfig state.

  Powering on or powering off an I/O chassis *resets the cell* to which it is connected (if any). Follow the same guidelines for power cycling I/O chassis that you follow for power cycling cells.

S620

Tools for Managing nPartition Booting

HP nPartition servers support the following software tools for booting and resetting nPartitions and for configuring and managing nPartition boot settings.

These tools overlap in some of the functionality they provide, but each has unique capabilities.

The primary tools for managing nPartition booting are shown below.

- **Service Processor (GSP or MP)**—Using a server complex's service processor menus, you can reset partitions, put partitions into the ready for reconfig state, and TOC the partitions in the complex.

  The service processor also provides power on and power off commands for power cycling server hardware components.

- **Virtual Front Panel (VFP)**—Each nPartition has its own VFP that displays current cell and partition boot states and activities.

  For each server complex you also can access a system VFP that gives a live partition boot state and activity status for all nPartitions in the complex.

- **Boot Console Handler (BCH)**—Each partition's BCH interface provides commands for booting HP-UX, rebooting the partition, and putting the partition into the ready for reconfig state.

  You also can configure boot-related settings and check the partition's hardware and boot-setting configurations using BCH menus.

- **HP-UX System Loaders (ISL and hpux)**—You can use system loaders to list files that reside on a boot device, such as kernel files in /stand, and can specify boot arguments to the hpux loader.

  You can access the ISL and hpux loaders after issuing the BCH interface's BOOT command, when BCH gives you the following option:

  ```
  Do you wish to stop at the ISL prompt prior to booting?
  (y/n)
  ```

  Replying "n" (no, do not stop at ISL) skips the ISL prompt and proceeds to execute the AUTO file, which by default will boot HP-UX (/stand/vmunix) on the nPartition.

ISL: Initial System Loader

Replying "y" (yes, do stop at ISL) allows you to interact directly with a boot device's Initial System Loader (ISL) and the Secondary System Loader (hpux). Enter all ISL commands from the `ISL>` prompt.

hpux: Secondary System Loader

From the ISL prompt you also can enter commands that are executed by the Secondary System Loader (hpux). Preface your Secondary System Loader command with **hpux**. For example: `hpux ls /stand` to list the contents of the /stand directory on the booted device.

See the *isl* (1M) and *hpux* (1M) manpages for details.

- **HP-UX utilities**—Several HP-UX utilities allow you to check and set a partition's HP-UX boot options; check the boot settings of other partitions in the server complex; and perform reboot, shutdown, and reboot for reconfig tasks.

  The `reboot`, `shutdown`, `parmodify`, `parstatus`, and `setboot` commands provide these features. For details see the command manpages.

  The Partition Manager utility (`/opt/parmgr/bin/parmgr`) also provides some boot configuration capabilities; details are available in its online help.

S622

Configurable Boot Settings

Each nPartition has its own collection of boot-related settings that specify which hardware manages the boot process (the core cell), how the boot process proceeds (automatically boot HP-UX, or wait for BCH commands), and whether cells are configured as active cells when the nPartition boots.

nPartition boot settings are stored as part of the server Complex Profile data.

You can configure each nPartition's boot settings by using the nPartition's BCH interface or by running HP-UX utilities on the nPartition.

By using the `parmodify` HP-UX command or Partition Manager, you also can configure some boot settings for remote (non-local) nPartitions in the same server complex.

You can reconfigure boot settings at any time to change the nPartition's boot behavior, specify different boot devices, or adjust settings based on nPartition configuration changes. Some boot setting changes require rebooting to take effect.

Also see *Checklist and Guidelines for Booting nPartitions* on page 184 for details on ensuring a bootable nPartition configuration.

You can configure the following boot settings for each nPartition: boot device paths, boot actions, core cell choices, cell use-on-next-boot value.

- **Boot Device Paths**

  You can set boot device paths to reference the hardware paths where bootable devices reside within the local nPartition.

  The boot device paths include the primary boot device (PRI boot path), the high-availability alternate device (HAA boot path, such as a mirror of the root volume), and the alternate device (ALT boot path, such as an install or recovery device).

  The PRI path is the default device booted by the BCH interface's `BOOT` command.

  You can set boot paths using the BCH interface, the `parmodify` command, and Partition Manager. The `setboot` command can set the PRI and ALT paths only.

5621

- **Boot Actions**

  Each boot device path has an associated boot action, which is established by the path's "path flag" setting. The boot actions (path flag settings) are referenced automatically when an nPartition initially boots to the BCH interface.

  Boot actions have no effect on boot behavior when you manually boot HP-UX using the BCH interface's BOOT command.

  The boot action for the PRI boot path establishes what the nPartition does when it boots and first reaches the BCH interface: boot the PRI device, go to the BCH Main menu, or skip the PRI path and attempt to perform the HAA path's boot action. You also can specify what action to take if an attempt to boot a device fails (either go to BCH, or try the next path).

  Depending on the PRI path flag setting, the HAA boot action may be referenced. Likewise, the HAA setting determines whether the ALT boot actions may be referenced.

  You can set boot actions using the BCH Configuration menu's PathFlags (PF) command. The setboot command can configure only the PRI actions from HP-UX.

  For details use the BCH Command menu's HELP PF command.

  You can stop an nPartition from automatically booting, and instead access the nPartition's BCH interface, by typing a key within ten seconds of the nPartition booting to BCH.

```
Primary Boot Path:  0/0/1/0/0.8
     Boot Actions:  Boot from this path.
                    If unsuccessful, go to BCH.

...

Attempting to boot using the primary path.
-------------------------------------------------------------

 To discontinue, press any key within 10 seconds.
```

- **Core Cell Choices**

  The core cell is the cell that "runs" the nPartition before it boots HP-UX. A processor on the core cell serves as the monarch processor that runs Boot Console Handler (BCH). The core cell is the one whose core I/O is active for the nPartition.

5620

One cell is selected as the **active core cell** for the nPartition when the nPartition boots. By default, the lowest numbered eligible cell in the nPartition is chosen. To be eligible the cell must: be active, have a connection to functioning core I/O, and be assigned to the nPartition.

You can designate up to four **core cell choices**, which are considered in the order you specify as candidates to be selected as the active core cell for the nPartition.

If none of the core cell choices is eligible to serve as the core cell, then the nPartition attempts to select a core cell using the default algorithm (lowest numbered eligible cell).

When no active cell in an nPartition can be selected, the nPartition will remain at the ready for reconfig state and cannot boot to BCH.

- **Use-on-Next-Boot Value for a Cell**

  Each cell in an nPartition has an associated *use-on-next-boot* value that determines whether the cell's resources are used by the nPartition.

  This setting does not affect the cell's nPartition assignment. The use-on-next-boot value only determines whether the cell is an *active* or *inactive* member of the nPartition when the nPartition boots.

  When a cell's use-on-next-boot value is "y" (use the cell), the cell can participate in nPartition rendezvous and become an *active* member of the nPartition, which enables its processors, memory, and any connected I/O to be made available for use by the nPartition.

  When a cell has a use-on-next-boot value of "n" (do not use the cell), the cell cannot participate in partition rendezvous so it will be an *inactive* member of the nPartition when the nPartition boots: all processors, memory, and I/O will not be made available.

  After changing a cell's use-on-next-boot value you might need to reset the nPartition so that all cells have a chance to either participate in partition rendezvous or remain inactive at BIB. (For example, if the nPartition is in the ready for reconfig state, just boot it using the service processor Command menu's `BO` command; but if the nPartition is active and has booted HP-UX then perform a reboot for reconfig using the `shutdown -R` command.)

  The use-on-next-boot setting does not directly affect the nPartition's boot behavior, but it will cause I/O connected to a cell to be unavailable when the cell boots with a "n" use-on-next-boot value.

5619

For details on configure these boot-related settings for an nPartition refer to the chapter *Booting and Resetting nPartitions* on page 197.

S618

Listing nPartition Boot Settings

You can list an nPartition's boot-related settings by using the nPartition's BCH interface or by using HP-UX commands.

To *list boot settings* for nPartitions, use the following procedures:

- *Listing nPartition Boot Settings [BCH]* on page 178
- *Listing nPartition Boot Settings [HP-UX]* on page 181
- *Listing nPartition Boot Settings [Partition Manager]* on page 183

Also see the following sections for details on *configuring boot settings* for nPartitions.

- *Configuring Boot Paths and Boot Actions* on page 227
- *Configuring Autoboot and Autostart* on page 233
- *Configuring Automatic System Restart for an nPartition* on page 235
- *Configuring Fast Boot Settings (Self Tests) for an nPartition* on page 238
- *Boot Timer Configuration for an nPartition* on page 242

Listing nPartition Boot Settings [BCH]

Use BCH commands from the **Main menu, Information menu**, and **Configuration menu** to list an nPartition's boot settings.

Step 1. Login to the server complex's service processor (GSP or MP), access the nPartition's console, and access the BCH Main menu.

From the nPartition console you access the nPartition's BCH interface. If the nPartition is not at the BCH interface, you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

Step 2. Access the BCH menu that provides the information you want to list.

The BCH interface's **Main menu, Information menu**, and **Configuration menu** provide commands for listing (and setting) boot options for the nPartition.

5617

- **BCH Main menu**

  If you are at one of the other BCH menus, enter **MA** to return to the BCH interface's Main menu.

Table 4-1 **BCH Main Menu Boot Settings**

PATH	Displays or sets the boot paths: primary (PRI), high-availability (HAA), and alternate (ALT).

- **BCH Configuration menu**

  From the BCH main menu, enter **CO** to access the Configuration menu.

Table 4-2 **BCH Configuration Menu Boot Settings**

AU	*Supported on HP Superdome servers only.* Displays or sets the auto-start flag, which determines whether the boot process proceeds following a self-test failure.
BOOTTIMER	Displays or sets the time allowed for booting.
CELLCONFIG	Displays or sets the (de)configuration of cells.
CORECELL	Displays or sets the core cell choices.
FASTBOOT	Displays or specifies whether certain self-tests are run during the boot process.
PATHFLAGS	Displays or sets the boot action for each boot path.

- **BCH Information menu**

  From the BCH Main menu, enter **IN** to access the Information menu.

Table 4-3 **BCH Information Menu Boot Settings**

BOOTINFO	Displays boot configuration information.

Step 3. At the appropriate BCH menu, issue the command to display the boot information of interest to you.

See the list in the previous step for commands and menus. Enter the command *with no arguments* to display (but not change) the boot setting.

S616

The following example shows using the PATH command to list the nPartition's boot paths, then accessing the BCH Configuration menu and issuing the PATHFLAGS command to list the nPartition's boot action settings for the PRI, HAA, and ALT boot paths.

```
Main Menu: Enter command or menu > PATH

     Primary Boot Path:  4/0/2/0/0.10
                         4/0/2/0/0.a     (hex)

HA Alternate Boot Path:  4/0/1/0/0.6
                         4/0/1/0/0.6     (hex)

   Alternate Boot Path:  4/0/1/0/0.5
                         4/0/1/0/0.5     (hex)

Main Menu: Enter command or menu > CO

---- Configuration Menu ------------------------------------

....

Configuration Menu: Enter command > PATHFLAGS

     Primary Boot Path Action
          Boot Actions:  Boot from this path.
                         If unsuccessful, go to next path.

HA Alternate Boot Path Action
          Boot Actions:  Boot from this path.
                         If unsuccessful, go to BCH.

   Alternate Boot Path Action
          Boot Actions:  Skip this path.
                         Go to BCH.

Configuration Menu: Enter command >
```

5615
21

Listing nPartition Boot Settings [HP-UX]

Use the **parstatus -V -p#** and **setboot** commands to list an nPartition's boot settings from HP-UX 11i.

NOTE Use the parstatus command to list various nPartition boot settings for *any* nPartition in a server complex.

The setboot command only provides information about the *local nPartition's* PRI and ALT boot paths and PRI boot actions.

Step 1. Login to HP-UX running on an nPartition.

If you want to list autoboot settings for an nPartition, you must login to the nPartition. To list other details, such as boot paths and core cell settings, you can login to any nPartition.

Step 2. Issue the **parstatus -V -p#** command to list detailed information about the specified nPartition (-p#), including boot-related details.

The boot setting information that parstatus -V -p# reports is equivalent to the following BCH commands: PATH, CELLCONFIG, and CORECELL.

The following example lists detailed information for nPartition number 0, including the nPartition's boot path settings, its core cell information, and each cell's use-on-next-boot settings.

```
# parstatus -V -p0
[Partition]
Partition Number         : 0
Partition Name           : jules00
Status                   : active
IP address               : 0.0.0.0
Primary Boot Path        : 0/0/2/0/0.13.0
Alternate Boot Path      : 0/0/2/0/0.0.0
HA Alternate Boot Path   : 0/0/2/0/0.14.0
PDC Revision             : 6.0
IODCH Version            : 23664
CPU Speed                : 552 MHz
Core Cell                : cab0,cell0
Core Cell Alternate [1]: cab0,cell0
Core Cell Alternate [2]: cab0,cell2
```

S614

```
[Cell]
                        CPU     Memory                                Use
                        OK/     (GB)                          Core    On
Hardware   Actual       Deconf/ OK/                           Cell    Next Par
Location   Usage        Max     Deconf    Connected To        Capable Boot Num
========== ============ ======= ========= =================== ======= ==== ===
cab0,cell0 active core  4/0/4    2.0/ 0.0 cab0,bay0,chassis1  yes     yes  0
cab0,cell2 active base  4/0/4    2.0/ 0.0 cab0,bay1,chassis3  yes     yes  0

[Chassis]
                                        Core Connected  Par
Hardware Location   Usage               IO   To         Num
=================== ============ ==== ========== ===
cab0,bay0,chassis1  active       yes  cab0,cell0 0
cab0,bay1,chassis3  active       yes  cab0,cell2 0

#
```

As the above example shows, the primary (PRI) boot path is 0/0/2/0/0.13.0, the active core cell is cell 0, and the core cell choices are cell 0 (first preference) and cell 2 (second preference). Both of the nPartition's cells are set to be used ("yes") the next time the nPartition boots. Both cells are actively used ("active core" and "active base").

Step 3. Issue the **setboot** command to list the *local nPartition's* PRI and ALT (but not HAA) boot paths, and to list the boot actions for the PRI boot path.

```
# setboot
Primary bootpath : 0/0/2/0/0.13.0
Alternate bootpath : 0/0/2/0/0.0.0

Autoboot is ON (enabled)
Autosearch is OFF (disabled)

Note: The interpretation of Autoboot and Autosearch has changed
for
systems that support hardware partitions. Please refer to the
manpage.
#
```

The setboot command reports the local nPartition's PRI and ALT boot path values, but does not list the HAA boot path.

The setboot command also reports the "autoboot" and "autosearch" settings for the PRI boot path. Combined, these two settings are equivalent to the PRI path's boot actions (its "path flags" setting).

S613
21

When autoboot is set to ON, the nPartition attempts to automatically boot from the PRI boot path when it first boots to BCH. Otherwise, when autoboot is OFF, the nPartition remains at the BCH interface on startup.

When autosearch is set to ON, the nPartition will attempt to perform the boot action for the HAA boot path if the PRI boot action is automatically attempted and fails to boot (when autoboot is ON). When autosearch is set to OFF, the nPartition remains at BCH if the PRI path is not automatically booted on startup.

Refer to the section *Configuring Autoboot and Autostart* on page 233 for other details and procedures.

Listing nPartition Boot Settings [Partition Manager]

This procedure (**Partition —> Show Partition Details** action, **General** tab) lists an nPartition's boot paths from Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. Select the nPartition whose boot path settings you want to view.

Partitions are listed on the left side of the Partition Manager primary window.

Step 3. Select the **Partition —> Show Partition Details** action and view the boot path settings in the **General** tab.

This displays the PRI, HAA, and ALT boot path values for the selected nPartition.

Checklist and Guidelines for Booting nPartitions

This section provides both a checklist to use when booting an nPartition, and a set of guidelines to consider when configuring nPartition boot settings.

Boot Checklist for nPartitions

Before you boot an nPartition, check the items listed here.

- ❑ All cells in the nPartition that have a "y" use-on-next-boot value should be powered on.

  If any cells that are set to be used are powered off, the nPartition will take longer to boot.

  During partition rendezvous, the nPartition will wait up to *10 minutes* for all cells that are designated to be used. Any cells not powered on will not be active or available in the nPartition.

- ❑ All I/O chassis and devices for the nPartition's active cells should be powered on.

- ❑ If any cells that have a "y" use-on-next-boot value are inactive, perform a reboot for reconfig of the nPartition (`shutdown -R`) to allow them to reset and become active during partition rendezvous.

- ❑ All complex profile information for the nPartition must be coherent.

  This means all cells assigned to the nPartition must have identical complex profile information (Partition Configuration Data).

  After you add a cell or remove and active cell from an nPartition, you must perform a reboot for reconfig of the nPartition (`shutdown -R`) to synchronize the complex profile data throughout the nPartition. The reboot for reconfig also causes all the nPartition's cells to reboot and allows cells to go through the partition rendezvous procedure.

Boot Configuration Guidelines for nPartitions

The following guidelines are points to consider when configuring boot settings for the nPartitions in your server complex.

- ❑ Configure HAA and ALT boot devices in addition to the PRI device.

By configuring HAA and ALT boot device paths, you establish additional bootable devices that provide redundancy in case the PRI device fails.

Also configure the path flags for the boot paths, to allow the HAA device to boot automatically if the device at the PRI path cannot boot.

- ❑ Ensure that the core I/O, PRI boot device, and network card(s) all are connected to same cell (the core cell).

  This configuration ensures that the core cell is directly connected to the I/O required for booting the nPartition and providing network connections. Having such a configuration eliminates the requirement for multiple cells to be functional to provide basic nPartition services.

- ❑ Have multiple core cells available within each nPartition, if possible.

  In order to have multiple core cell choices, the nPartition must have at least two cells, each connected to an I/O chassis and core I/O.

  Having such a configuration provides redundancy and potentially improved system availability. If one core cell has a failure or otherwise cannot serve as the active core cell, the second core-capable cell can serve as the active core cell.

  Disregard this guideline if configuring multiple nPartitions in an HP rp7405 / rp7410 or HP rp8400 server complex. HP rp7405/rp7410 servers and HP rp8400 servers have up to two core-capable cells only, so following this guideline would require having only one nPartition in the server complex.

S610

nPartition Boot Activity Monitoring

On HP nPartition servers you can monitor the nPartition boot process—from power-on or reset to HP-UX start-up—using the Virtual Front Panel (VFP) view of the nPartition.

Each nPartition has its own VFP that displays details about the nPartition's cells and the nPartition's boot state and activity.

NOTE After you add or remove cells from the nPartition, you must exit and re-enter the nPartition's VFP to update the list of cells the VFP displays.

Monitoring nPartition Boot Activity [Service Processor]

Use the following procedure (service processor Main menu, **VFP** option) to access an nPartition Virtual Front Panel for monitoring the nPartition's boot status.

Step 1. From the Main menu, enter **VFP** to select the Virtual Front Panel option.

```
 GSP MAIN MENU:

Utility Subsystem FW Revision Level: SR_XXXX_D

          CO: Consoles
         VFP: Virtual Front Panel
          CM: Command Menu
          CL: Console Logs
          SL: Show chassis Logs
          HE: Help
           X: Exit Connection

GSP> VFP
```

If you are accessing the service processor using a single-partition-user account, selecting the VFP option takes you directly to the nPartition's Virtual Front Panel.

If accessing the GSP using an operator or administrator account, you can select the VFP for any single nPartition, or can select a *system VFP* that displays the nPartition state and activity for all nPartitions within the server complex.

Step 2. Select the nPartition you wish to monitor.

Skip this step if you are accessing the service processor using a single-partition-user account.

```
 Partition VFP's available:

        #    Name
       ---   ----
        0)   jules00
        1)   jules01
        S)   System (all chassis codes)
        Q)   Quit

GSP:VFP> 1
```

Step 3. View the VFP details for information about the nPartition and its current boot state.

To exit the VFP and return to the service processor main menu, type **^b** (**Control-b**).

The VFP provides information about the nPartition state, nPartition activity, each cell's state, and each cell's activity. The VFP display updates as the cell or nPartition state and activities change.

```
E indicates error since last boot
     Partition 1  state                Activity
     ------------------                --------
     Cell(s) Booting:     57 Logs

  #  Cell state                        Activity
  -  ----------                        --------
  4  Booting                           Cell firmware test                   28  Logs
  6  Booting                           Cell firmware test                   28  Logs


GSP:VFP (^B to Quit) >
```

5608

Hanged HP-UX and Running HP-UX Detection

This section describes how you can determine whether HP-UX still is running on an nPartition even when you are unable to login or access the nPartition console.

You also may wish to reference the information in the procedure *Configuring Automatic System Restart for an nPartition* on page 235 for details on configuring an nPartition to reboot when HP-UX has hanged on it for over three minutes.

Detecting if HP-UX is Running or Hanged on an nPartition

To determine whether HP-UX is running or has hanged on an nPartition use this procedure (first check the Virtual Front Panel, then check the Chassis Logs menu's **Live Logs** display, then the nPartition's Console).

Refer to the chapter *Using Console and Service Processor Interfaces* on page 125 for details on service processor login accounts and features.

Step 1. Access and view the nPartition's Virtual Front Panel (VFP).

Login to the service processor (GSP or MP) for the server where the nPartition resides, enter `VFP` to access the VFP menu, and select the nPartition whose boot state you want to check.

- To exit an nPartition's VFP, type **^b** (**Control-b**).
- When HP-UX has booted on the nPartition, `HPUX heartbeat` is displayed as the partition state when you view the nPartition VFP.
- If HP-UX is alive, an asterisk (`*`) blinks on and off in the partition state area of the nPartition VFP.

Also see *Boot States and Activities for nPartitions and Cells* on page 194 for details interpreting the VFP status.

Step 2. If the nPartition VFP indicates that HP-UX has booted but is not alive, exit the VFP and view the live chassis logs for the nPartition.

At the GSP main menu, enter `SL` to enter the **Show chassis Logs** menu, and enter `L` to select the **Live Chassis Logs** display from the **Chassis Logs** menu.

S607

```
GSP> SL

Chassis Logs available:

     (A)ctivity Log
     (E)rror Log
     (L)ive Chassis Logs

     (C)lear All Chassis Logs
     (Q)uit

GSP:VW> L

         Entering Live Log display
```

Step 3. From the Live Log display, type **P** and select the nPartition whose chassis codes you want to view by typing the partition number.

By default the live chassis log viewer only displays alert codes.

When you select the partition filter, the live log's view changes to show all codes for the selected nPartition.

```
         Entering Live Log display

         A)lert filter
         C)ell filter
         P)artition filter
         U)nfiltered
         V)iew format selection
         ^B to Quit

Current filter: ALERTS only

P
Enter partition number to display

    Partitions available:
     #   Name
    ---  ----
     0)  feshd4a
     2)  feshd4b
     Q)  Quit
    Please select partition number: 0

Filtering partition 0
```

Step 4. When viewing the selected nPartition's live log display, determine whether HP-UX is emitting HEARTBEAT chassis codes.

To exit the live log display, type **^b** (**Control-b**)

Heartbeat for HP-UX

When HP-UX is running on the nPartition, the live log partition filter shows the nPartition's HP-UX HEARTBEAT chassis codes and corresponding ACTIVITY_LEVEL_TIMEOUT counter updates.

```
Filtering partition 0
Alert Level 0: No failure; Keyword: HEARTBEAT
Processor 0 ; Status: 15
Logged by HP-UX 26 during display_activity update subActivity 10
Legacy PA HEX chassis-code: f10f
0xf8e1a8001100f10f 0x000000000000f10f

HPUX 0,0,0   0  ACTIVITY_LEVEL_TIMEOUT
Alert Level 0: No failure; Keyword: ACTIVITY_LEVEL_TIMEOUT
Processor 0 timeout; Status:  0
Logged by HP-UX 0 during display_activity update subActivity 0
Activity Level/Timeout: 0% / 3 minutes
0x78e008041100f000 0x0000000200000000

HPUX 0,6,2   0  HEARTBEAT
Alert Level 0: No failure; Keyword: HEARTBEAT
Processor 0 ; Status: 15
Logged by HP-UX 26 during display_activity update subActivity 10
Legacy PA HEX chassis-code: f10f
0xf8e1a8001100f10f 0x000000000000f10f
```

Activity Timeout Counter

The nPartition activity timeout counter is reset every time HP-UX on the nPartition emits a HEARTBEAT chassis code. The timeout counter expires when no HEARTBEAT code has been emitted for three minutes in the nPartition.

See *Configuring Automatic System Restart for an nPartition* on page 235 for more details about the activity timeout counter.

Step 5. If the nPartition is not emitting HEARTBEAT chassis codes, then access the nPartition's console by entering **CO** from the service processor main menu and selecting the partition number for the nPartition.

Accessing the nPartition's console may help determine whether an HP-UX crash dump is occurring or any console or error messages were given.

5605

Step 6. Determine whether the nPartition needs to be reset in order to restore HP-UX to a running state.

Review the findings from the previous steps in this procedure.

HP-UX on the nPartition may be considered “hanged” if you observed all of the following VFP, live log, and console behaviors:

- The VFP indicates `HPUX heartbeat` in the partition state with no asterisk (`*`) blinking to indicate activity.
- The nPartition’s live log displays no `HEARTBEAT` chassis codes.
- The nPartition console is inactive with no indication of a crash dump or other error, and no console login or interactivity is possible.

If all of the above attempts to find signs of HP-UX activity on the nPartition fail, then you may need to reset the nPartition before HP-UX can be restored to a running state.

For details see the procedure *Rebooting or Resetting an nPartition* on page 214 or the procedure *Performing a Transfer-of-Control (TOC) Reset of an nPartition* on page 223.

5604

Troubleshooting Boot Issues

On HP nPartition servers, you might encounter different boot issues than on other HP servers.

The following boot issues are possible on nPartition servers.

- **Problem:** Not all cells boot to join (rendezvous) an nPartition.

  Causes: Some cells may have their use-on-next-boot value set to "n" (do not use), or the cells may have been powered off, or the cells may have booted too late to participate in partition rendezvous, or the cells have failed self-tests and cannot be used.

  Actions: Check the cell use-on-next-boot values and change them to "y" as needed then reboot for reconfig (`shutdown -R`). Check cell power (`frupower -d -C`) and power on any cells as needed, then reboot for reconfig.

  As the nPartition's cells reboot, observe the boot progress from the nPartition's VFP and note any problems the cells have proceeding from one boot state to the next; as needed review chassis logs and error logs using the service processor Show Chassis Logs (`SL`) menu.

- **Problem:** An nPartition takes a long time to boot (over ten minutes).

  Causes: One or more cells assigned to the nPartition that have a "y" use-on-next-boot value has not booted to participate in partition rendezvous, thus causing the rest of the nPartition's cells to wait for ten minutes for the cell to report.

  For example, the cell might not be installed, might be powered off, or might have been powered on or reset too late to rendezvous with the other cells.

  Actions: You can avoid the delay by performing any of the following actions, as needed. Perform a reboot for reconfig following any changes you make.

  — Set the cell's use-on-next-boot value to "n" (do not use).

  — Power on the cell.

  — Unassign (remove) the cell from the nPartition.

5603

- **Problem:** An nPartition does not boot to BCH and instead all cells remain at a boot-is-blocked (BIB) state.

  Causes: The nPartition has been reset to the ready for reconfig state, or no valid core cell is available to the nPartition.

  Actions: If the nPartition was reset to the ready for reconfig state, use the service processor Command menu's BO command to boot the nPartition base boot-is-blocked (to allow it to boot to its BCH interface).

  If no valid core cell was available to the nPartition when it booted, check the power for all core cell choices (a cell might be powered off) and power it on if needed.

  Also review the chassis logs for the nPartition to search for any core cell problems and failures.

5602

Boot States and Activities for nPartitions and Cells

On HP nPartition servers, the cell and nPartition boot process proceeds from one boot state to the next; cells and nPartitions complete various boot activities within each boot state before proceeding to the next boot state.

You can view current details about nPartition and cells boot states and activities by viewing the nPartition's Virtual Front Panel. From the service processor (GSP or MP) Main menu enter **VFP** to access the VFPs that are available for the server complex.

Table 4-4 on page 195 presents the nPartition and cell states and activities that you can observe from an nPartition's Virtual Front Panel.

You can view a Virtual Front Panel for a specific nPartition that includes details for all cells in the nPartition, as shown below.

```
E indicates error since last boot
     Partition 0  state              Activity
     ------------------              --------
     Cell(s) Booting:    904 Logs

  #  Cell state                      Activity
  -  ----------                      --------
  0  Late CPU selftest               Processor test                       299   Logs
  2  Late CPU selftest               Processor test                       299   Logs
  4  Memory discovery                Physical memory test                 304   Logs




GSP:VFP (^B to Quit) >
```

You also can view a system-wide VFP, which shows a summary of each nPartition's current state and its activity.

569

Inactive cells remain at a “Boot Is Blocked (BIB)” state following I/O discovery and do not participate in partition rendezvous.

Table 4-4 **HP nPartition and Cell Boot States and Activities**

Partition State	Partition Activity	Cell States	Cell Activities
Cell(s) Booting		Booting	Cell firmware configuration, Cell firmware test, Cell PDH controller configuration
Cell(s) Booting		Early CPU self-test	Processor test, Cell firmware test, Processor firmware slave rendezvous
Cell(s) Booting		Memory discovery	Physical memory test
Cell(s) Booting		Late CPU self-test	Processor test, Cell firmware test, Processor firmware slave rendezvous
Cell(s) Booting		I/O discovery	I/O system bus adapter configuration, I/O local bus adapter configuration
Cell(s) Booting		Remote fabric initialization	Partition rendezvous slave rendezvous
Memory Interleave	Memory controller configuration	Cell has joined partition	
At Boot Console Handler (BCH)	Partition firmware	Cell has joined partition	
ISL Menu		Cell has joined partition	
HPUX Loader Init		Cell has joined partition	

Table 4-4 HP nPartition and Cell Boot States and Activities (Continued)

Partition State	Partition Activity	Cell States	Cell Activities
HPUX Launch	Processor system initialization	Cell has joined partition	
HPUX Launch	Partition IPL launch configuration	Cell has joined partition	
HPUX Launch	Processor display_activity update	Cell has joined partition	
HPUX init process start		Cell has joined partition	
HPUX heartbeat		Cell has joined partition	

559a

5 Booting and Resetting nPartitions

This chapter presents procedures for booting and resetting nPartitions and procedures for configuring an nPartition's boot-related options.

For an introduction to nPartition boot issues, refer to the chapter *An Overview of nPartition Boot and Reset* on page 161.

NOTE For details on booting and rebooting virtual partitions within an nPartition, refer to the chapter *Virtual Partitions (vPars) Management on nPartitions* on page 441.

Accessing an nPartition Console and BCH Interface

Each nPartition has its own Boot Console Handler (BCH) interface that provides you a method for interacting with the nPartition before HP-UX has booted on it.

You must access an nPartition's console and BCH interfaces through the server complex's service processor (GSP or MP). See *Accessing nPartition Console and BCH Interfaces [Service Processor]* below for a detailed procedure.

On nPartition servers, each nPartition's BCH interface is available through the nPartition's console before HP-UX has booted. The BCH interface enables you to manage the nPartition's HP-UX boot process and to configure various boot-related settings.

NOTE

Always login to a server complex's service processor from a tty (not console) login session. You can check your current login terminal using the **`who -m`** command.

Do not login to a service processor from an nPartition console connection. Any use of the **^b** (**Control-b**) console exit sequence would exit the original console login—not the subsequent console-based login to the service processor—thus potentially stranding the console-based login (for example, if it too were accessing a console).

Accessing nPartition Console and BCH Interfaces [Service Processor]

The following procedure (login to service processor, select Console menu, select an nPartition) accesses an nPartition's console and BCH interface using the server complex's service processor.

Step 1. Login to the service processor (the GSP or MP) for the nPartition's server complex.

You can connect to the service processor using a direct physical connection, or using `telnet` for a remote connection.

ss97

In most situations, you can `telnet` to the service processor.

```
# telnet sdome-s
Trying...
Connected to sdome-s.rsn.hp.com.
Escape character is '^]'.
Local flow control off

GSP login: Accountname
GSP password:

                              Welcome to
               Superdome's Guardian Service Processor
```

Step 2. Select the Console menu (`CO`) from the service processor's Main menu.

The Console menu is the method for accessing nPartition consoles.

```
 GSP MAIN MENU:

Utility Subsystem FW Revision Level: SR_XXXX_D

            CO: Consoles
           VFP: Virtual Front Panel
            CM: Command Menu
            CL: Console Logs
            SL: Show chassis Logs
            HE: Help
             X: Exit Connection

GSP> CO
```

If you are accessing the service processor using a single-partition-user account, selecting the `CO` (console) option takes you directly to the nPartition's console.

If using an operator or administrator account, you can access the console for any of the nPartitions within the server complex.

Step 3. At the Console menu, enter the partition number for the nPartition whose console (and BCH interface) you wish to access.

Skip this step if you are accessing the service processor using a single-partition-user account.

If using an operator or administrator account, select the nPartition whose console you wish to access.

```
GSP> CO

    Partitions available:

     #    Name
    ---   ----
     0)   jules00
     1)   jules01
     Q)   Quit

    Please select partition number: 1

        Connecting to Console: jules01

        (Use ^B to return to main menu.)

        [A few lines of context from the console log:]

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

     SERvice menu                      Displays service commands

     DIsplay                           Redisplay the current menu
     HElp [<menu>|<command>]           Display help for menu or command
     REBOOT                            Restart Partition
     RECONFIGRESET                     Reset to allow Reconfig Complex Profile
----
Main Menu: Enter command or menu >

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

The console displays the last 10 lines of console output when you connect to it. This provides you a view of the most recent console activity.

Step 4. Gain interactive access to the nPartition console.

Press **Enter** to access the nPartition console's currently available prompt, if any. You will have either interactive or non-interactive access, as described in the sections *Interactive Console Access* and *Non-Interactive Console Access* in this step.

To exit the nPartition console and return to the service processor Main menu, type **^b** (**Control-b**) at any time.

Interactive Console Access

Typically the BCH interface, ISL interface, or the HP-UX login or command prompt is available from the nPartition console.

- **When an nPartition is at the BCH interface** you can access BCH commands from the nPartition's console and can reboot BCH if needed.
- **When an nPartition has booted to ISL** you can use the `EXIT` command to exit ISL and return to the nPartition's BCH interface.
- **When an nPartition has booted HP-UX**, in order to access the BCH interface you must reboot HP-UX and if necessary interrupt the automatic boot process. (To reboot the nPartition, use the `shutdown -r` command, or use `shutdown -R` if you also are changing the nPartition's cell configuration.)

Non-Interactive Console Access

In the following situations, you cannot interact with the nPartition's console. In these cases you can wait until the console is interactive or can force interactive access.

- **When the nPartition is resetting or is booting HP-UX** you cannot interact with software running on the nPartition.

  Once the nPartition has completed resetting, or has completed booting HP-UX, you can interact with the nPartition's BCH or HP-UX prompts.

  To determine an nPartition's boot state, use the nPartition's Virtual Front Panel (the VFP menu, available from the service processor Main menu).

- **When another user already is attached to the console** you can access the nPartition's console in spy (read-only) mode or can force write access by typing `^ecf` (**Control-e c f**).

  Spy mode allows you to view console information but does not enable you to enter commands. If you type when accessing an nPartition console in spy mode, the console prints the following message.

  ```
  [Read-only - use ^Ecf to attach to console.]
  ```

  When in spy mode, you can force access to the nPartition's console by typing `^ecf` (**Control-e c f**). Doing this provides you interactive console access and forces ("bumps") the user who was using the console into spy mode.

  ```
  [Bumped user - Admin.]
  ```

Boot Device Searching and Finding

You can search for and find bootable devices for an nPartition by using the BCH interface's SEARCH command. This command searches for and reports all bootable devices connected to any of the nPartition's currently active cells.

NOTE

You cannot access any I/O connected to an nPartition's *inactive* cells (cells not being used for the current nPartition boot) or cells *not assigned* to the local nPartition.

As a consequence, the BCH SEARCH command does not report any devices connected to cells that are not currently assigned and active in the local nPartition.

Finding Bootable Devices [BCH]

This procedure (BCH Main menu, SEARCH command) finds and lists the bootable devices that are available to an nPartition.

Step 1. Login to the server complex's service processor (GSP or MP) and access the nPartition's console.

From the nPartition console you access the nPartition's BCH interface to search for bootable devices.

If the nPartition is not at the BCH interface you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

Step 2. From the BCH interface's Main menu, issue the SEARCH command to find and list bootable devices in the nPartition.

When accessing the nPartition's BCH interface, if you are not at the BCH Main menu then enter MA to return to the Main menu.

The SEARCH command reports all potential boot devices it locates.

```
---- Main Menu ---------------------------------------------------------------

     Command                             Description
     -------                             -----------
     BOot [PRI|HAA|ALT|<path>]           Boot from specified path
```

```
        PAth [PRI|HAA|ALT] [<path>]       Display or modify a path
        SEArch [ALL|<path>]               Search for boot devices
        ScRoll [ON|OFF]                   Display or change scrolling capability

        COnfiguration menu                Displays or sets boot values
        INformation menu                  Displays hardware information
        SERvice menu                      Displays service commands

        DIsplay                           Redisplay the current menu
        HElp [<menu>|<command>]           Display help for menu or command
        REBOOT                            Restart Partition
        RECONFIGRESET                     Reset to allow Reconfig Complex Profile
----
Main Menu: Enter command or menu > SEARCH

Searching for potential boot device(s)
This may take several minutes.

To discontinue search, press any key (termination may not be immediate).

   Path#  Device Path (dec)                       Device Type
   -----  -----------------                       -----------
   P0     0/0/1/0/0.15                            Random access media
   P1     0/0/1/0/0.12                            Random access media
   P2     0/0/1/0/0.11                            Random access media
   P3     0/0/1/0/0.9                             Random access media
   P4     0/0/1/0/0.8                             Random access media
   P5     0/0/1/0/0.6                             Random access media

Main Menu: Enter command or menu >
```

The SEARCH command lists up to the first 20 potential boot devices that it locates, and lists each with a path number (P0 through P19).

To boot a device that was reported by the SEARCH command, specify the path number or the full device path. For example, BOOT P0 would boot the path listed as path number P0.

HP-UX Booting on an nPartition

nPartitions boot and reboot HP-UX independently from each other. This section describes how to boot a single instance of HP-UX on an nPartition.

NOTE For details on booting HP-UX in virtual partitions (vPars), refer to the section *Booting HP-UX on Virtual Partitions* on page 487.

You can boot HP-UX on an nPartition using the BCH interface's BOOT command.

Each nPartition's BCH interface is available through its console. All nPartition consoles are available from the complex's service processor (GSP or MP) Console menu.

An nPartition will *automatically boot HP-UX* when its boot paths (PRI, HAA, ALT) and corresponding boot actions are appropriately set. For details see *Configuring Boot Paths and Boot Actions* on page 227.

On HP Superdome servers only, if one of the nPartition's components fails self-test and AUTOSTART is OFF then the nPartition stops booting at the BCH interface.

Booting HP-UX on an nPartition [BCH]

The following procedure (BCH interface **BOOT** command) boots HP-UX on an nPartition using the nPartition's BCH interface.

Step 1. Login to the server complex's service processor (GSP or MP), access the nPartition's console, and access the BCH Main menu.

From the nPartition console, you access the nPartition's BCH interface.

If the nPartition is not at the BCH interface, you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

When accessing the nPartition's BCH interface, if you are not at the BCH Main menu then enter MA to return to the Main menu.

Step 2. Choose which device you wish to boot.

From the BCH Main menu, use the PATH command to list any boot path variable settings. The primary (PRI) boot path normally is set to the main boot device for the nPartition. You also can use the SEARCH command to find and list potentially bootable devices for the nPartition.

```
Main Menu: Enter command or menu > PATH

     Primary Boot Path:  0/0/2/0/0.13
                         0/0/2/0/0.d     (hex)

HA Alternate Boot Path:  0/0/2/0/0.14
                         0/0/2/0/0.e     (hex)

   Alternate Boot Path:  0/0/2/0/0.0
                         0/0/2/0/0.0     (hex)

Main Menu: Enter command or menu >
```

Step 3. Boot the device using the BCH interface's **BOOT** command.

You can issue the BOOT command in any of the following ways:

- **BOOT**

  Issuing the BOOT command with no arguments boots the device at the primary (PRI) boot path.

BOOT *bootvariable*

  This command boots the device indicated by the specified boot path, where *bootvariable* is the PRI, HAA, or ALT boot path.

  For example, BOOT PRI boots the primary boot path.

- **BOOT LAN INSTALL** or **BOOT LAN.*ip-address* INSTALL**

  The BOOT... INSTALL commands boot HP-UX from the default HP-UX install server or from the server specified by *ip-address*.

BOOT *path*

  This command boots the device at the specified *path*. You can specify the *path* in HP-UX hardware path notation (for example, 0/0/2/0/0.13) or in "path label" format (for example, P0 or P1) .

  If you specify the *path* in "path label" format then *path* refers to a device path reported by the last SEARCH command.

After you issue the BOOT command, the BCH interface prompts you to specify whether you want to stop at the ISL prompt.

To boot the /stand/vmunix HP-UX kernel from the device *without stopping at the ISL prompt*, enter **n** to automatically proceed past ISL and execute the contents of the AUTO file on the selected device. (By default the AUTO file is configured to load /stand/vmunix.)

```
Main Menu: Enter command or menu > BOOT PRI

     Primary Boot Path:  0/0/1/0/0.15


 Do you wish to stop at the ISL prompt prior to booting? (y/n)
 >> n


ISL booting  hpux

Boot
: disk(0/0/1/0/0.15.0.0.0.0.0;0)/stand/vmunix
```

To boot an HP-UX kernel other than /stand/vmunix, or to boot HP-UX in single-user or LVM-maintenance mode, stop at the ISL prompt and specify the appropriate arguments to the hpux loader.

558
2X

Booting an nPartition to the ISL Prompt

When you issue the BCH interface's BOOT command, you can stop an nPartition's booting at the Initial System Loader (ISL) interface in order to interact with the ISL prompt.

To exit ISL and return to the BCH interface, enter the EXIT command at the ISL prompt. For help enter HELP at the ISL prompt.

Normally you will not need to access ISL unless you need to use the Secondary System Loader (hpux).

For details about ISL, see the *isl* (1M) manpage. Details on the Secondary System Loader (hpux) are in the *hpux* (1M) manpage.

NOTE On HP nPartition servers many of the ISL commands *are not supported*. For example, AUTOBOOT, AUTOSEARCH, and PRIMPATH are not supported at ISL.

These and other features are instead supported on HP nPartition servers by each nPartition's BCH interface.

Booting an nPartition to ISL [BCH]

This procedure (BCH BOOT command, and reply **y** to "stop at the ISL prompt") boots an nPartition to the ISL prompt.

Step 1. Login to the server complex's service processor (GSP or MP), access the nPartition's console, and access the BCH interface.

From the nPartition console, you access the nPartition's BCH interface. If the nPartition is not at the BCH interface you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

If an nPartition is configured to automatically boot HP-UX, you must interrupt the boot process before HP-UX boots, then manually boot HP-UX using the BOOT command (in the next step) to access the ISL interface on the nPartition.

Step 2. Boot the desired device using the BCH interface's **BOOT** command, and specify that the nPartition stop at the ISL prompt prior to booting (reply **y** to the "stop at the ISL prompt" question).

The EXIT command exits ISL and returns to the nPartition BCH interface, and the HELP command lists all available ISL interface commands.

```
Main Menu: Enter command or menu > BOOT 0/0/2/0/0.13

 BCH Directed Boot Path: 0/0/2/0/0.13


 Do you wish to stop at the ISL prompt prior to booting? (y/n)
>> Y

Initializing boot Device.


ISL Revision A.00.42  JUN 19, 1999

ISL>
```

Single-User or LVM-Maintenance Mode HP-UX Booting

On an nPartition you can boot HP-UX in single-user mode or LVM-maintenance mode by specifying options to the Secondary System Loader (hpux).

From the nPartition's console, use the BCH interface to boot the desired device and stop at the Initial System Loader (ISL) interface, then use the Secondary System Loader (hpux) to specify the options for booting HP-UX in the desired mode.

See the *hpux* (1M) manpage for details on using the Secondary System Loader (hpux).

Booting HP-UX in Single-User or LVM-Maintenance Mode [BCH, ISL, and hpux]

This procedure (BCH **BOOT** command, stop at ISL interface, use hpux loader with options) boots HP-UX in single-user mode or LVM-maintenance mode on an nPartition.

Step 1. Login to the server complex's service processor (GSP or MP), access the nPartition's console, and access the BCH interface.

From the nPartition console you access the nPartition's BCH interface. If the nPartition is not at the BCH interface you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

Step 2. Boot the desired device using the BCH interface's **BOOT** command, and specify that the nPartition stop at the ISL prompt prior to booting (reply **y** to the "stop at the ISL prompt" question).

```
Main Menu: Enter command or menu > BOOT 0/0/2/0/0.13

 BCH Directed Boot Path: 0/0/2/0/0.13


 Do you wish to stop at the ISL prompt prior to booting? (y/n)
>> y

Initializing boot Device.

....
```

586

```
ISL Revision A.00.42  JUN 19, 1999

ISL>
```

Step 3. From the ISL prompt, issue the appropriate Secondary System Loader (hpux) command to boot the HP-UX kernel in the desired mode.

Use the hpux loader to specify the boot mode options and to specify which kernel (such as: /stand/vmunix) to boot on the nPartition.

- To boot HP-UX in single-user mode:

  ```
  ISL> hpux -is boot /stand/vmunix
  ```

- To boot HP-UX in LVM-maintenance mode:

  ```
  ISL> hpux -lm boot /stand/vmunix
  ```

- To boot HP-UX at the default run level:

  ```
  ISL> hpux boot /stand/vmunix
  ```

To exit the ISL prompt and return to the BCH interface, issue the `EXIT` command instead of specifying one of the above hpux loader commands.

See the *hpux* (1M) manpage for a detailed list of hpux loader options.

Example 5-1 **Example Single-User HP-UX Boot**

```
ISL Revision A.00.42  JUN 19, 1999

ISL> hpux -is /stand/vmunix

Boot
: disk(0/0/2/0/0.13.0.0.0.0.0;0)/stand/vmunix
8241152 + 1736704 + 1402336 start 0x21a0e8

....

INIT: Overriding default level with level 's'

INIT: SINGLE USER MODE

INIT: Running /sbin/sh
#
```

5585

HP-UX Install Source Booting

You can boot an nPartition from an HP-UX installation source—such as an install CD or an Ignite server—by specifying the install source using the BCH interface's BOOT command.

This allows you to install HP-UX on any of the nPartition's eligible devices.

NOTE For instructions on installing HP-UX, refer to the book *HP-UX 11i Installation and Update Guide*, which is supplied with the HP-UX operating environment media.

Booting from an HP-UX Install Source [BCH]

This procedure boots an HP-UX install source on an nPartition using the nPartition's BCH interface.

Step 1. Login to the server complex's service processor (GSP or MP), access the nPartition's console, and access the BCH interface.

From the nPartition console, you access the nPartition's BCH interface. If the nPartition is not at the BCH interface you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

Step 2. Select the HP-UX install source that you wish to boot.

From the BCH main menu, you can boot from an Ignite server or install CD-ROM in order to install HP-UX.

You can use the SEARCH command to find and list potentially bootable devices for the nPartition, including any DVD-ROM devices that may have CD-ROM install media. The ALT boot path also might be set to the DVD-ROM device's path.

Step 3. Boot the install source using the BCH interface's **BOOT** command.

Specify the device path where the install media resides or specify the install server.

For details on booting, see *HP-UX Booting on an nPartition* on page 204.

Shutting Down HP-UX on an nPartition

When HP-UX is running on an nPartition, you can shut down HP-UX using either the `shutdown` command or the `reset` command.

NOTE The `reboot` command does not invoke the shutdown scripts associated with subsystems. The `shutdown` command invokes the scripts and terminates all running processes in an orderly and cautious manner.

On nPartitions you have the following options when shutting down HP-UX:

- To shut down HP-UX and **reboot** an nPartition: **`shutdown -r`**
- To shut down HP-UX and **halt** an nPartition: **`shutdown -h`**
- To perform a **reboot for reconfig** of an nPartition: **`shutdown -R`**
- To hold an nPartition at a **ready for reconfig** state: **`shutdown -R -H`**

For details see the *shutdown* (1M) manpage.

Shutting Down HP-UX on an nPartition [HP-UX]

This procedure shuts down HP-UX on an nPartition.

Step 1. Login to HP-UX running on the nPartition.

You can login to HP-UX on the nPartition either by directly connecting (with the `telnet` or `rlogin` commands) or by logging in to its complex's service processor (GSP or MP) and using the Console menu to access the nPartition's console.

Accessing the console through the service processor allows you to maintain console access to the nPartition after HP-UX has shut down.

Step 2. Issue the **`shutdown`** command with the appropriate command-line options.

The command-line options you specify dictate the way in which HP-UX is shut down, whether the nPartition is rebooted, and whether any nPartition configuration changes (adding or removing cells) take place.

Use the following list to choose an HP-UX shut down option for your nPartition.

- Shut down HP-UX and halt the nPartition.

  Issue the `shutdown -h` command to shut down and halt the nPartition.

  This leaves the nPartition and all its cells in an *active* state (the nPartition cannot be reconfigured) after HP-UX shuts down and halts.

  To reboot the nPartition you must reset the nPartition using the GSP command menu's `RS` command.

- Shut down HP-UX and reboot the nPartition.

  Issue the `shutdown -r` command to shut down and reboot the nPartition.

- Perform a *reboot for reconfig* of the nPartition.

  Issue the `shutdown -R` command to perform a reboot for reconfig.

  This shuts down HP-UX, reconfigures the nPartition if needed, and reboots the nPartition.

- Reboot the nPartition and put it in to the *ready for reconfig* state.

  Use the `shutdown -R -H` command to hold the nPartition in the ready for reconfig state.

  This leaves the nPartition and all its cells in an *inactive* state (the nPartition can be reconfigured remotely).

  To reboot the nPartition you must do so manually by using the service processor Command menu's `BO` command.

If HP-UX is halted on the nPartition, thus not allowing you to use the `shutdown` command, you can reboot or reset the nPartition by issuing commands from the service processor Command menu.

See *Rebooting or Resetting an nPartition* on page 214.

5587

Rebooting or Resetting an nPartition

When you perform a reboot or reset of an nPartition, all *active cells* in the nPartition reboot and return to BCH or HP-UX. Any *inactive* cells in the nPartition are not rebooted in this procedure.

You can reset and reboot an nPartition by using these procedures:

- *Rebooting or Resetting an nPartition [Service Processor]* on page 215
- *Rebooting or Resetting an nPartition [BCH]* on page 216
- *Rebooting or Resetting an nPartition [HP-UX]* on page 216

NOTE If possible you should down HP-UX before resetting an nPartition.

HP's nPartition servers also support other types of nPartition resetting.

See the following sections for details on these other nPartition reset methods:

- *Shutting Down HP-UX on an nPartition* on page 212
- *Performing a Reboot for Reconfig for an nPartition* on page 218
- *Holding an nPartition at the Ready for Reconfig State* on page 219
- *Performing a Transfer-of-Control (TOC) Reset of an nPartition* on page 223

Rebooting or Resetting an nPartition [Service Processor]

Use the service processor Command menu **RS** command to reset an nPartition from the service processor (GSP or MP).

Step 1. Login to the server complex's service processor (GSP or MP) and access the Command menu.

After logging in to the service processor, enter **CM** to select the Command menu.

```
GSP login: Accountname
GSP password: Password

....

GSP> CM

                     Enter HE to get a list of available commands

GSP:CM>
```

Step 2. At the Command menu, enter the **RS** command, specify which nPartition is to be reset, and confirm whether to reset it.

The Command menu's RS command resets all *active cells* in the nPartition and reboots them past partition rendezvous to BCH or HP-UX.

Be certain to correctly select which nPartition to be reset.

```
GSP:CM> RS

This command resets the selected partition.

WARNING: Execution of this command irrecoverably halts all
system
         processing and I/O activity and restarts the selected
         partition.


    #    Name
   ---   ----
    0)   jules00
    1)   jules01

   Select a partition number: 1

   Do you want to reset partition number 1? (Y/[N]) y
```

5580

```
    -> The selected partition will be reset.
GSP:CM>
```

If you are accessing the service processor using a single-partition-user account, the RS command selects which nPartition is to be reset: the nPartition that your account allows you to access.

If using an operator or administrator service processor account, you can select which of the server complex's nPartitions you want to reset.

Rebooting or Resetting an nPartition [BCH]

Use the **REBOOT** command to reset an nPartition from the BCH interface.

Step 1. Login to the server complex's service processor, access the nPartition's console, and access the BCH Main menu.

From the nPartition console you access the nPartition's BCH interface. If the nPartition is not at the BCH interface you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

Step 2. From the nPartition's BCH main menu, enter the **REBOOT** command to reboot the nPartition.

The BCH interface's REBOOT command resets all *active cells* in the nPartition and reboots them past partition rendezvous to BCH or HP-UX.

```
Main Menu: Enter command or menu > REBOOT
Rebooting the partition ...
```

Rebooting or Resetting an nPartition [HP-UX]

Use the **shutdown -r** command to reset an nPartition from HP-UX running on the nPartition.

Step 1. Login to HP-UX running on the nPartition you want to reset.

You can login to HP-UX on the nPartition either by directly connecting (with the telnet or rlogin commands) or by logging in to its complex's service processor (GSP or MP) and using the Console menu to access the nPartition's console.

Step 2. Issue the **shutdown -r** command to reset the nPartition.

The `shutdown -r` command shuts down HP-UX and reboots the nPartition. All *active cells* in the nPartition are reset.

Performing a Reboot for Reconfig for an nPartition

During a **reboot for reconfig** of an nPartition, the HP-UX command that you issue (`shutdown -R`) performs the following tasks:

1. Shuts down HP-UX and resets all cells that are assigned to the nPartition, including any inactive cells.
2. Reconfigures the nPartition if necessary (adds or removes cells).
3. Boots all cells in the nPartition. Any cells with a “n” use-on-next-boot value remain inactive at BIB, and all other cells can rendezvous to form the nPartition.

You should perform a reboot for reconfig of an nPartition whenever you add or remove cells from the nPartition, and whenever you need to allow an inactive cell to join the nPartition (such as after changing a cell’s use-on-next-boot value from “n” to “y”).

Performing a Reboot for Reconfig [HP-UX]

Use the **`shutdown -R`** command to perform a reboot for reconfig for an nPartition.

Step 1. Login to HP-UX running on the nPartition.

You can login to HP-UX on the nPartition either by directly connecting (with the `telnet` or `rlogin` commands) or by logging in to its complex’s service processor (GSP or MP) and using the Console menu to access the nPartition’s console.

Step 2. Issue the **`shutdown -R`** command to perform a reboot for reconfig of the nPartition.

The `shutdown -R` command shuts down HP-UX, reboot all cells assigned to the nPartition, performs any nPartition reconfigurations, and boot all cells that have “y” use-on-next-boot values.

5577

Holding an nPartition at the Ready for Reconfig State

Resetting an nPartition to the **ready for reconfig** state performs any changes to the nPartition's configuration and holds the nPartition and all its cells in a boot-is-blocked (*inactive*) state.

To boot an nPartition after you have reset it to the ready for reconfig state, you must use the service processor (GSP or MP) Command menu's `BO` command.

You can hold an nPartition at the ready for reconfig state by using the following procedures:

- *Holding an nPartition at the Ready for Reconfig State [Service Processor]* on page 220
- *Holding an nPartition at the Ready for Reconfig State [BCH]* on page 221
- *Holding an nPartition at the Ready for Reconfig State [HP-UX]* on page 221

When you use the above methods to hold an nPartition at the ready for reconfig state, the commands perform the following tasks:

1. Shut down HP-UX (if using the `shutdown -R -H` command) and reset all cells that are assigned to the nPartition, including any inactive cells.
2. Reconfigures the nPartition if necessary (adds or removes cells).
3. Keeps all cells at a boot-is-blocked state; the nPartition and all cells assigned to it are inactive.

You should reset an nPartition to ready for reconfig whenever you need for the nPartition and its cells to be inactive. This enables you to modify the nPartition's configuration from the GSP or from HP-UX running on a remote nPartition in the same system complex.

Holding an nPartition at the Ready for Reconfig State [Service Processor]

Use the Command menu **RR** command to reset an nPartition to the ready for reconfig state from the service processor (GSP or MP).

Step 1. Login to the server complex's service processor and enter **CM** to access the Command menu.

```
GSP> CM

                                Enter HE to get a list of available commands

GSP:CM>
```

Step 2. At the service processor Command menu, enter the **RR** command, specify which nPartition is to be reset, and confirm whether to reset it to the ready for reconfig state.

The service processor's RR command resets all cells in the nPartition, performs any nPartition reconfigurations, and halts all cells at a boot-is-blocked state, thus making the nPartition and all its cells inactive.

Be certain to select the correct nPartition to be reset.

```
GSP:CM> RR

This command resets for reconfiguration the selected partition.

WARNING: Execution of this command irrecoverably halts all system
         processing and I/O activity and restarts the selected
         partition in a way that it can be reconfigured.


        #    Name
       ---   ----
        0)   jules00
        1)   jules01

    Select a partition number: 1


    Do you want to reset for reconfiguration partition number 1? (Y/[N]) y

    -> The selected partition will be reset for reconfiguration.
GSP:CM>
```

If you are accessing the service processor using a single-partition-user account, the RR command selects which nPartition is to be reset: the nPartition that your account allows you to access.

If using an operator or administrator GSP account, you can select which of the server complex's nPartitions you want to reset.

Holding an nPartition at the Ready for Reconfig State [BCH]

Use the **RECONFIGRESET** command to reset an nPartition to the ready for reconfig state from the nPartition's BCH interface.

Step 1. Login to the server complex's service processor, access the nPartition's console, and access the BCH interface.

From the nPartition console you access the nPartition's BCH interface. If the nPartition is not at the BCH interface you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

Step 2. From the nPartition's BCH interface, enter the **RECONFIGRESET** command to reset the nPartition to the ready for reconfig state.

The RECONFIGRESET command resets all cells in the nPartition, performs any nPartition reconfigurations, and halts all cells at a boot-is-blocked state, thus making the nPartition and all its cells inactive.

```
Main Menu: Enter command or menu > RECONFIGRESET
Reset the partition for reconfiguration of Complex Profile ...
```

Holding an nPartition at the Ready for Reconfig State [HP-UX]

Use the **shutdown -R -H** command to reset an nPartition to the ready for reconfig state from HP-UX running on the nPartition.

Step 1. Login to HP-UX running on the nPartition.

You can login to HP-UX on the nPartition either by directly connecting (with the `telnet` or `rlogin` commands) or by logging in to its complex's service processor (GSP or MP) and using the Console menu to access the nPartition's console.

Step 2. Issue the **shutdown -R -H** command to reset the nPartition to the ready for reconfig state.

The `shutdown -R -H` command shuts down HP-UX, reset all cells in the nPartition, perform any nPartition reconfigurations, and halt all cells at a boot-is-blocked state, thus making the nPartition and all its cells inactive.

Performing a Transfer-of-Control (TOC) Reset of an nPartition

You can use the service processor Command menu's `TC` command to perform a transfer-of-control (TOC) reset of an nPartition.

If crash dump is configured for HP-UX on the nPartition, when you TOC the nPartition while it is running HP-UX the nPartition performs a crash dump and gives you an opportunity select the type of dump.

Performing a TOC Reset of an nPartition [Service Processor]

Use the Command menu **`TC`** command to perform a transfer-of-control (TOC) reset of an nPartition.

Step 1. Login to the server complex's service processor and enter **`CM`** to access the Command menu.

```
GSP> CM

                    Enter HE to get a list of available commands

GSP:CM>
```

Step 2. At the Command menu, enter the **`TC`** command, specify which nPartition is to be reset, and confirm whether to TOC the nPartition.

The `TC` command performs a transfer-of-control reset on the specified nPartition.

If you are accessing the service processor using a single-partition-user account, the `TC` command selects which nPartition is to be reset: the nPartition that your account allows you to access.

If using an operator or administrator account, you can select which of the server complex's nPartitions you want to TOC.

Be certain to select the correct nPartition to be reset.

```
GSP:CM> TC

This command TOCs the selected partition.
```

```
WARNING: Execution of this command irrecoverably halts all system
         processing and I/O activity and restarts the selected
         partition.


     #   Name
    ---  ----
     0)  jules00
     1)  jules01

Select a partition number: 0

    Do you want to TOC partition number 0? (Y/[N]) y

    -> The selected partition will be TOCed.
GSP:CM>
```

Step 3. After you initiate the TOC, you can observe its progress and select the type of crash dump through the nPartition's console.

Once the nPartition completes the dump, or once you cancel it, the nPartition reboots.

```
       ******* Unexpected TOC. Processor HPA FFFFFFFF'FC07C000 *******
                              GENERAL REGISTERS:
r00/03 00000000'00000000 00000000'0099CA2C 00000000'00000000 00000000'010BB790
r04/07 00000000'00000002 00000000'010BC140 00000000'0080F000 00000000'00AA2490
r08/11 00000000'00000001 00000000'0099A800 00000000'0099A800 00000000'0099C800

....

Processor 8 TOC:  pcsq.pcoq = 0'0.0'12675c
                  isr.ior   = 0'10340004.0'2f8bfd30

Boot device reset done.
*** The dump will be a SELECTIVE dump:  457 of 4080 megabytes.
*** To change this dump type, press any key within 10 seconds.
*** Proceeding with selective dump.

*** The dump may be aborted at any time by pressing ESC.
*** Dumping:   7% complete (32 of 457 MB) (device 64:0x2)
```

Booting an Inactive nPartition past Boot-Is-Blocked (BIB)

When all cells in an nPartition are at boot-is-blocked, the nPartition is *inactive*. This is the case, for example, when an nPartition is held at the ready for reconfig state.

You can boot an nPartition past the ready for reconfig state to make it active by using the service processor Command menu's BO (boot) command.

To determine whether an nPartition is in a boot-is-blocked (ready for reconfig) state, use the nPartition's Virtual Front Panel to monitor the nPartition's boot activity. If all of the nPartition's cells are at boot-is-blocked, the nPartition is halted at the ready for reconfig state.

Booting an Inactive nPartition past BIB [Service Processor]

Use the service processor Command menu **BO** command to boot an nPartition past the ready for reconfig state to make the nPartition active.

If you use the Command menu's BO command to attempt to boot an nPartition that already is active, the command has no effect.

Step 1. Login to the server complex's service processor and enter **CM** to select the Command menu.

```
# telnet sdome-s
Trying...
Connected to sdome-s.rsn.hp.com.
Escape character is '^]'.
Local flow control off

GSP login: Accountname
GSP password: Password

....

GSP> CM

                    Enter HE to get a list of available commands


GSP:CM>
```

Step 2. From the Command menu, enter the BO command and specify which nPartition is to be booted (released from boot-is-blocked).

As a result of the BO command, the complex's service processor releases the selected nPartition's cells from boot-is-blocked: the cells proceed to rendezvous to form an active nPartition, which no longer is in the ready for reconfig state.

```
GSP:CM> BO

This command boots the selected partition.


     #    Name
    ---   ----
     0)   jules00
     1)   jules01

    Select a partition number: 0

    Do you want to boot partition number 0? (Y/[N]) y

    -> The selected partition will be booted.
GSP:CM>
```

Any of the nPartition's cells that are not configured (those with a "n" use-on-next-boot value) remain inactive at boot-is-blocked.

When the nPartition becomes active it proceeds through the normal boot process and performs, as necessary, the boot action set for each of the boot paths (PRI, HAA, ALT).

SS69

Configuring Boot Paths and Boot Actions

You can configure each nPartition's boot *paths* (device paths for booting HP-UX) and boot *actions* (preferred automatic boot behavior) by using the following procedures:

- *Configuring Boot Paths and Actions [BCH]* on page 229
- *Configuring Boot Paths and Actions [HP-UX]* on page 230

By configuring boot paths and boot actions for an nPartition, you can set the nPartition to automatically boot from a primary source or, if the primary source fails, from backup devices.

Each nPartition's **boot device paths** list the hardware paths of devices for booting HP-UX on the nPartition.

The boot paths are:

- PRI—Primary boot path.
- HAA—High-availability alternate boot path, typically a mirror of the primary root volume.
- ALT—Alternate boot path. Typically used for install or recovery media (such as DAT or CD-ROM drive).

Each nPartition also has a set of **boot actions (path flags)**, which specify the *default actions to be automatically performed* when the nPartition boots to the BCH interface. Each of the three boot paths (PRI, HAA, and ALT) has its own path flag setting that defines its boot action.

The order in which an nPartition's boot actions are attempted is: PRI boot action, then HAA boot action (if necessary), and finally ALT boot action (if necessary).

The boot actions (path flag settings) for each boot path are:

- 0—Go to BCH.
- 1—Boot this path, if fail go to BCH.
- 2—Boot this path, if fail attempt to perform the next path's boot action.
- 3—Skip this path, attempt to perform the next path's boot action.

By default, all path flags are set to 0 ("Go to BCH").

The boot actions are performed *automatically* by the BCH interface when an nPartition boots to BCH, as possible and necessary. However, boot action settings *do not* affect the behavior of the BCH BOOT command.

Setting Autoboot through Boot Paths and Boot Actions

Each nPartition's **Autoboot setting** is established by the boot action (path flag) settings for the nPartition's boot paths.

For an nPartition to *automatically boot HP-UX*, it must be configured in the following way:

- The nPartition must have at least one bootable HP-UX device that is pointed to by the PRI, HAA, or ALT boot path variable.
- The path flag (boot action) setting for a bootable device's path variable must be set to "boot this path" (1 or 2).
- When the nPartition boots it must proceed to execute a bootable device's boot action that specifies to "boot this path", and it must find the device.

For example, an nPartition could automatically boot HP-UX with the following configuration: both the PRI and HAA paths point to bootable devices, and the PRI action is 2 ("boot this path, if fail attempt to perform the next path's boot action") and the HAA action is 1 ("boot this path, if fail go to BCH").

In this example configuration, the nPartition could automatically boot HP-UX even if the PRI path were not available. When the nPartition boots to BCH it first attempts to boot the PRI device. If the PRI device cannot be booted, because the PRI path flag specifies to "if fail attempt to perform the next path's boot action", it then refers to the HAA path and action. Because in this example the HAA path points to a bootable device, and because the HAA path flag specifies to attempt to boot the HAA device, the nPartition can still automatically boot HP-UX (if the HAA device is available).

Configuring Boot Paths and Actions [BCH]

Use the BCH Main menu **PATH** command and Configuration menu **PATHFLAGS** command to configure an nPartition's boot paths and boot actions (path flags) through its BCH interface.

To list all boot path and action settings for an nPartition, you also can use the BCH Information menu's BOOTINFO command.

Step 1. Determine which devices will be used for booting HP-UX on the nPartition, and determine the boot behaviors you desire.

You need to determine the hardware paths of all potential boot devices that you will configure as the PRI, HAA, and ALT boot paths.

You also need to determine which device you want to boot by default (if any), and which (if any) device you want to boot if the default device fails to boot.

Typically, the PRI path is set to the default boot device and the HAA path is set to the device you want to boot if PRI fails to boot.

Step 2. Login to the service processor (GSP or MP), access the nPartition's console, and access the BCH Main menu.

From the nPartition console you access the nPartition's BCH interface. If the nPartition is not at the BCH interface you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

Step 3. At the BCH Main menu, set the boot path values using the **PATH** command.

To list the current boot path settings, enter **PATH** with no arguments.

To set a boot path, enter **PATH** ***VAR hwpath***, where *VAR* is the boot path variable (PRI, HAA, or ALT) and *hwpath* is a boot device's hardware path.

For example, to set the PRI boot path to a new value (4/0/2/0/0.10, in this case) enter PATH PRI 4/0/2/0/0.10, as shown below.

```
Main Menu: Enter command or menu > PATH PRI 4/0/2/0/0.10.0

    Primary Boot Path:  4/0/2/0/0.10
                        4/0/2/0/0.a    (hex)

Main Menu: Enter command or menu >
```

SS66

Step 4. Access the BCH Configuration menu by entering **CO** at the Main menu, and set the boot action for each boot path, as desired, by using the **PATHFLAGS** command.

At the BCH Configuration menu, you can list the path flags (boot actions) for all boot path variables by entering **PATHFLAGS** with no arguments.

To set the boot action for each of the boot paths, enter **PATHFLAGS** ***VAR action***, where *VAR* is the boot path variable (PRI, HAA, or ALT) and *action* is the boot action (0 for "go to BCH", 1 for "boot, if fail go to BCH", 2 for "boot, if fail try next path", or 3 for "skip this path, try next path").

For example, to configure an nPartition to boot from the PRI device or (if PRI fails to boot) the HAA device, use the following two BCH Configuration commands: **PATHFLAGS PRI 2** and **PATHFLAGS HAA 1**, as shown below.

```
Configuration Menu: Enter command > PATHFLAGS PRI 2

     Primary Boot Path Action
          Boot Actions:  Boot from this path.
                         If unsuccessful, go to next path.

Configuration Menu: Enter command > PATHFLAGS HAA 1

HA Alternate Boot Path Action
          Boot Actions:  Boot from this path.
                         If unsuccessful, go to BCH.

Configuration Menu: Enter command >
```

For other help in setting path flags, enter HELP PATHFLAGS at the BCH Configuration menu prompt.

Configuring Boot Paths and Actions [HP-UX]

Use the **parmodify -p#...** and **setboot...** commands to set nPartition boot path variables from HP-UX and to check and set the local nPartition's PRI boot action (the PRI path flag).

Step 1. Determine which devices will be used for booting HP-UX on the nPartition, and determine the boot behaviors you desire for the PRI boot path.

5565

Step 2. Login to HP-UX running on an nPartition in the complex.

You can modify the boot paths for any nPartition from any other nPartition in the complex when using the `parmodify` command.

However, when using the `setboot` command to modify the PRI and ALT paths or the PRI boot action, you can modify only the *local* nPartition's settings.

Step 3. Configure boot path settings using the **`parmodify -p#...`** command.

Use the following commands to set the boot path variables for a specified partition number (`-p#`):

- PRI path— `parmodify -p# -b` *`PRI`* where *`PRI`* is the hardware path.
- HAA path—`parmodify -p# -s` *`HAA`* where *`HAA`* is the hardware path.
- ALT path—`parmodify -p# -t` *`ALT`* where *`ALT`* is the hardware path.

If using the `setboot` command to set boot paths for the *local nPartition*, you can specify `setboot -p` *`PRI`* or `setboot -a` *`ALT`* but cannot set the HAA path variable.

You can list an nPartition's current boot path settings by issuing the `parstatus -V -p# | grep Path` command and specifying the partition number (`-p#`). The `setboot` command with no arguments lists the PRI and ALT settings for the local nPartition as well as the local nPartition's PRI path flags (boot actions).

For example, to set the PRI boot path to 0/0/4/0/0.8.0 and the HAA boot path to 0/0/4/0/0.9.0 for partition number 0, issue the `parmodify -p0 -b 0/0/4/0/0.8.0 -s 0/0/4/0/0.9.0` command, as shown below.

```
# parmodify -p0 -b 0/0/4/0/0.8.0 -s 0/0/4/0/0.9.0
Command succeeded.
#
```

Step 4. As needed, configure the PRI boot action for the *local nPartition* by using the **`setboot -b`** ***`Autoboot`*** **`-s`** ***`Autosearch`*** command.

The `setboot` command supports the following options for setting local nPartition boot actions:

`-b` **Autoboot setting** for the local nPartition:

`-b on` to automatically boot the PRI path.

`-b off` to not boot PRI.

`-s` **Autosearch setting** for the local nPartition:

`-s on` to attempt to perform the HAA path's boot action when PRI is not booted (either when `-b` is `off`, or when PRI fails to boot when `-b` is on).

`-s off` to never attempt to perform the HAA action.

For example, to always stop the local nPartition at BCH when booting, issue the `setboot -b off -s off` command.

See *Setting Autoboot through Boot Paths and Boot Actions* on page 228 or the *setboot* (1M) manpage for details.

Configuring Autoboot and Autostart

The **Autoboot setting** specifies whether an nPartition automatically boots HP-UX. You can configure each nPartition's Autoboot setting by modifying the nPartition's boot actions for its boot paths. See the *Autoboot Configuration* section.

On HP Superdome servers only, you can configure an **Autostart setting** for each nPartition to specify the nPartition's boot behavior when one or more self tests fails. See the *Autostart Configuration* section that follows.

Autoboot Configuration

Each nPartition's Autoboot setting is established by a combination of its boot path variable settings and the settings for each path's boot actions (determined by its path flags).

You can use the BCH Main menu's PATH command and the BCH Configuration menu's PATHFLAGS command to set boot paths and boot actions for an nPartition. You also can use the `parmodify` and `setboot` HP-UX commands to configure some of the boot path and action settings.

See *Configuring Boot Paths and Boot Actions* on page 227 for details on configuring these settings to enable Autoboot.

Autostart Configuration

On HP Superdome servers only, the BCH interface's Autostart setting for each nPartition determines the boot behavior when one of the nPartition's components (processors or memory) fails self test.

By default Autostart is set to OFF, and the nPartition stops at the BCH interface when a processor or DIMM fails self-test.

When Autostart is ON, the nPartition proceeds with the normal boot process and performs the boot actions for its boot paths as necessary.

CSG2

Configuring Superdome nPartition Autostart [BCH]

Use the BCH Configuration menu's **AU** command to configure Autostart for an nPartition on an HP Superdome server.

NOTE This procedure applies to nPartitions on HP Superdome servers only.

Step 1. Login to the Superdome complex's service processor (GSP), access the nPartition's console, and access the BCH Configuration menu.

From the nPartition console, you can access the nPartition's BCH interface. If the nPartition is not at the BCH interface you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

From the BCH Main menu, enter **CO** to access the Configuration menu.

Step 2. From the BCH Configuration menu, use the **AU** command to list or set Autostart for the nPartition.

Enter **AU** with no arguments to list the Autostart setting.

Enter **AU ON** to set Autostart to ON, or **AU OFF** to set it to OFF.

5561

Configuring Automatic System Restart for an nPartition

The **automatic system restart** feature on nPartition servers enables you to configure an nPartition to be automatically rebooted when HP-UX hangs on the nPartition.

By default, automatic system restart *is disabled* for nPartitions.

To enable or disable automatic system restart, use the service processor Command menu's AR command, as described in *Configuring nPartition Automatic System Restart [Service Processor]* on page 236.

To use the AR command, you must login to the server complex's service processor using an account that has administrator authority.

CAUTION When automatic system restart is enabled for an nPartition, all cells in the nPartition automatically will be reset—and the nPartition will reboot—if HP-UX running on the nPartition is hung for three (3) minutes.

When HP-UX is booted on an nPartition, it indicates that it is "alive" by emitting a HEARTBEAT chassis code and an ACTIVITY_LEVEL_TIMEOUT chassis code approximately every four seconds.

The service processor manages automatic system restart for each nPartition through a timer that tracks the time since the nPartition was active. This timer is reset every time an ACTIVITY_LEVEL_TIMEOUT chassis code is emitted by HP-UX on the nPartition. If HP-UX does not emit this chassis code for three minutes then it emits an "Alert Level 13: System hang detected" chassis code. If the nPartition has automatic system restart enabled then the service processor issues a PARTITION_TIMEOUT_RESET chassis code, resets all cells assigned to the nPartition, and the nPartition reboots.

The following output shows the chassis codes (with keywords) for an HP-UX timeout and automatic reset.

SS60

```
129  GSP  0     *13 0x591008d1a000205f 0x000065060c0f1611 PARTITION_TIMEOUT_RESET
128  HPUX 0,0,0 *13 0x78e004d41100f000 0x0000000300000009
128  HPUX 0,0,0 *13 0x58e00c000000f000 0x000065060c0f1610 07/12/2001 15:22:16
```

Monitoring HP-UX Activity and Chassis Logs

You can monitor whether HP-UX is active on an nPartition through the nPartition's Virtual Front Panel and through the Chassis Logs viewer.

- You can track an nPartition's HP-UX activity through its Virtual Front Panel (VFP) display, which is available through the service processor. When HP-UX has booted on an nPartition, the nPartition's VFP blinks an HP-UX heartbeat indicator based on the HEARTBEAT chassis code.
- You also can track HP-UX activity though the service processor's Chassis Logs viewer, which enables you to view live (real-time) chassis codes as well as previously recorded error and activity chassis codes.

  For example, to monitor an nPartition's chassis codes in real time: from the service processor Main menu select `SL` for the Chassis Logs viewer, select the live chassis logs option, then type `P` and select which nPartition's chassis codes you want to monitor (to exit to the Main menu type **^b**).

Configuring nPartition Automatic System Restart [Service Processor]

Use the service processor Command menu's **AR** command to enable or disable automatic system restart for an nPartition.

Step 1. Login to the server complex's service processor (GSP or MP) and enter **CM** to access the Command menu.

Step 2. Issue the service processor Command menu's **AR** command to enable or disable automatic system restart for an nPartition.

To use the `AR` command, you must be logged in using an account that has administrator authority.

```
GSP:CM> AR

This command modifies the automatic system restart configuration of
the selected partition.
```

5559

```
         #   Name
        ---  ----
         0)  feshd5a
         1)  feshd5b

        Select a partition number: 0

        Automatic system restart for partition 0 is currently enabled.
        Do you want to disable automatic system restart? (Y/[N]) y

        -> Automatic system restart is disabled.
GSP:CM>
```

558

Configuring Fast Boot Settings (Self Tests) for an nPartition

The **fast boot settings** for an nPartition determine which self tests the nPartition performs during the power on or nPartition boot process.

You can configure nPartition fast boot settings by enabling and disabling various self tests using these procedures:

- *Configuring Fast Boot for an nPartition [BCH]* on page 239
- *Configuring Fast Boot for an nPartition [HP-UX]* on page 239

NOTE HP recommends that all self tests be performed for nPartitions.

When an nPartition reboots due to a system panic, HPMC, or TOC, all self tests are performed when the nPartition reboots.

On HP nPartition servers you can configure the following self tests:

- **PDH tests**—Processor-dependent hardware tests that test a checksum of read-only memory.

  Can be configured from BCH and HP-UX `setboot` as “PDH”.
- **Early CPU tests**—Firmware, cache, and CPU-specific tests that are performed out of firmware.

  Can be configured from BCH (as “EARLY”) and HP-UX `setboot` (as “early_cpu”).
- **Late CPU tests**—Firmware, cache, and CPU-specific tests that are performed out of memory and thus are faster than early CPU tests.

  Can be configured from BCH (as “LATE”) and HP-UX `setboot` (as “late_cpu”).

5557

Configuring Fast Boot for an nPartition [BCH]

Use the Configuration menu's FASTBOOT command to configure an nPartition's fast boot settings using its BCH interface.

Step 1. Login to the server complex's service processor (GSP or MP), access the nPartition's console, and access the BCH Configuration menu.

From the nPartition console you access the nPartition's BCH interface. If the nPartition is not at the BCH interface you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

From the BCH Main menu, enter `CO` to access the Configuration menu.

Step 2. At the BCH Configuration menu use the **`FASTBOOT`** command to list or set the nPartition's fast boot settings.

Enter `FASTBOOT` with no arguments to display the current fast boot settings. This lists which self tests are set to be performed or skipped.

NOTE HP recommends that *all self tests* be performed for all nPartitions.

To *enable all tests* for an nPartition, use the **`FASTBOOT RUN`** command at the nPartition's BCH Configuration menu.

To *disable* an individual test, enter `FASTBOOT` *`test`* `SKIP`, where *`test`* is the name of the self test ("PDH", "EARLY", or "LATE").

To *enable* an individual test, enter `FASTBOOT` *`test`* `RUN`.

For details on setting self tests, enter `HELP FASTBOOT` at the Configuration menu.

Configuring Fast Boot for an nPartition [HP-UX]

Use the **`setboot`** command to configure an nPartition's self test configuration from HP-UX running on the nPartition.

Step 1. Login to HP-UX running on the nPartition whose self test configuration you want to change.

From HP-UX you can configure self tests for the *local* nPartition only.

556

Step 2. Enter the **`setboot -v`** command to list the current self test configuration for the local nPartition.

The self test details listed by `setboot -v` include:

> TEST—The keyword names of self tests that you can enable or disable.
> CURRENT—The nPartition's setting for the test in stable storage: on means the test is normally executed on each boot, `off` means the test is normally omitted on each boot, `partial` means some subtests normally are executed on each boot. This may differ from the NEXT BOOT settings.
> SUPPORTED—Whether the server supports the test completely (yes), partially (`partial`), or not at all (no).
> DEFAULT—The default setting for the test, either on, `off`, or `partial`.
> NEXT BOOT—The nPartition's self test behavior for the *next boot only*. If these settings differ from CURRENT, then the CURRENT settings are reestablished after the next boot.

The following example shows `setboot -v` output for an nPartition.

```
# setboot -v
Primary bootpath : 0/0/6/0/0.6.0
Alternate bootpath : 0/0/1/0/0.8.0

Autoboot is OFF (disabled)
Autosearch is OFF (disabled)

Note: The interpretation of Autoboot and Autosearch has changed for
systems that support hardware partitions. Please refer to the manpage.
TEST            CURRENT        SUPPORTED      DEFAULT        NEXT BOOT
----            -------        ---------      -------        ---------
all             partial        partial        partial        partial
  SELFTESTS     on             yes            on             on
    early_cpu   on             yes            on             on
    late_cpu    on             yes            on             on
  FASTBOOT      partial        partial        partial        partial
    full_memory off            no             off            off
    PDH         on             yes            on             on
  CEC           off            no             off            off
#
```

Step 3. Use the **`setboot...`** command to enable or disable boot-time self tests for the local nPartition.

You can use the following commands to configure tests:

`setboot -t` *`test_name`*`=[on|off|default]`

`setboot -T` *`test_name`*`=[on|off|default]`

5585

`test_name` is the name of the self test (“PDH”, “early_cpu”, “late_cpu”) or is “all” (for all tests).

The `setboot` command’s `-t` option changes the test setting in stable storage and affects all following boots. The `-T` option changes the test setting for the next boot only.

NOTE HP recommends that *all self tests* be performed for all nPartitions.

To *enable all tests* for an nPartition, use the following command:
`setboot -t all=on`

For example, to enable the early CPU tests and PDH tests but disable the late CPU tests issue the following command:

```
setboot -t early_cpu=on -t PDH=on -t late_cpu=off
```

This changes the local nPartition’s settings for these tests in its stable storage and uses these test configurations for all following boots.

After modifying an nPartition’s self test configuration, you can list the new settings with the `setboot -v` command.

For more details see the *setboot* (1M) manpage.

5554

Boot Timer Configuration for an nPartition

The boot timer setting establishes the number of seconds an nPartition will wait for a boot device before timing out.

When a boot device does not respond to a boot request within the number of seconds defined by the boot timer setting, the boot is considered unsuccessful.

Configuring an nPartition Boot Timer [BCH]

Use the Configuration menu's **BOOTTIMER** command to configure an nPartition's boot timer setting from its BCH interface.

Step 1. Login to the server complex's service processor (GSP or MP), access the nPartition's console, and access the BCH Configuration menu.

From the nPartition console, you access the nPartition's BCH interface. If the nPartition is not at the BCH interface, you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

From the BCH Main menu, enter `CO` to access the Configuration menu.

Step 2. From the BCH Configuration menu, use the **BOOTTIMER** command to list or set the boot timer setting.

Enter `BOOTTIMER` with no arguments to list the current setting.

Enter `BOOTTIMER` *seconds* to set the boot timer setting to the specified (*seconds*) number of seconds.

SS53

21

6 Managing nPartitions

This chapter presents the procedures for creating, configuring, and managing nPartitions on HP servers that support them.

For an introduction to nPartition features, refer to the chapter *nPartition System Overviews* on page 31.

For nPartition configuration requirements and related HP recommendations, refer to the chapter *Planning nPartition Configurations* on page 109.

Coordinating Changes to nPartitions

When you modify nPartitions, you should perform your changes so that they occur at a time when they will not conflict with other nPartition changes in the same server complex.

The HP-UX nPartition configuration commands and the Partition Manager utility coordinate their actions by using *locks* to restrict access to portions of the server's *Complex Profile* data while they modify that data.

Commands and utilities can lock Stable Complex Configuration Data and Partition Configuration Data to ensure that only the command holding the lock can modify that portion of the Complex Profile.

In most cases, the nPartition commands and utilities will not have locking conflicts because they can complete changes quickly (within about a second), usually before any other commands attempt to modify the same portion of the server's Complex Profile data.

However, some nPartition changes involve locking parts of the Complex Profile for a longer time.

- The Partition Manager utility locks all parts of the server's Complex Profile that it may potentially modify, and it keeps them locked for as long as the associated menu items are being used.

  For example, the **Partition —> Create Partition** menu item and the **Complex —> Set Complex Name** menu item lock the Stable Complex Configuration Data portion of the server's Complex Profile. You cannot use other tools to perform any tasks that modify the Stable Complex Configuration Data (such as adding or removing cells) until the task that acquired the lock completes or is canceled.

  Likewise, the **Partition —> Modify Partition** menu item locks both the Stable Complex Configuration Data as well as the selected nPartition's Partition Configuration Data. As a result, no other tool (including another instance of Partition Manager) can add or remove cells or modify the selected nPartition until this task has completed or been canceled.

  Some tasks performed through Partition Manager also require performing a reboot for reconfig to release locks (for example, removing an active cell from an nPartition).

5551

- When *removing an active cell* from an nPartition, you must perform a reboot for reconfig (`shutdown -R`, not `-r`) of the modified nPartition to release the Complex Profile lock, regardless of whether you use `parmodify` or Partition Manager.

  You must perform the reboot for reconfig before you can add or remove other cells from nPartitions in the server complex. (The lock on the Stable Complex Configuration Data is not released in this case until the reboot for reconfig has occurred.)

- When you *add or remove cells from an active nPartition* and specify the `parmodify` command's `-B` option, the Stable Complex Configuration Data remains locked until the modified nPartition has performed a reboot for reconfig. In this situation, no further changes to cell assignments can occur until after the reboot for reconfig.

Although you can use the `parunlock` command to force-unlock any parts of a server's Complex Profile, you *should not use* this command unless the program that established the lock has abnormally terminated. Instead, if possible, you should allow the Complex Profile to be unlocked as part of the normal procedures described above. See the *parunlock* (1M) manpage for details.

5550

Rebooting to Implement nPartition Changes

Once an nPartition has booted and is active, the nPartition has a fixed set of active hardware resources. In order to establish a different set of active hardware resources for an nPartition you must reboot the nPartition, as described below.

You can add and remove cells from an active, booted nPartition; however, you only can add or remove *inactive* cells without having to reboot the nPartition.

To remove an active cell from an nPartition, or to make a newly added cell or inactive cell *active*, you must perform a reboot for reconfig of the nPartition.

The following list describes situations where you may need to reboot an nPartition to implement changes.

- Perform a reboot for reconfig (**`shutdown -R`**) of an nPartition in the following situations.
  - When you want to add one or more cells to an nPartition.

    Newly added cells initially are inactive when assigned to an nPartition. To allow the new cells to rendezvous (join the nPartition as active members), perform a reboot for reconfig.
  - When you remove one or more cells from an nPartition.

    Removing an active cell requires an nPartition reboot for reconfig, but removing an *inactive* cell *does not* require an nPartition reboot for reconfig. Inactive cells are removed immediately.
  - When you change a cell's use-on-next-boot value from "n" (no, do not use) to "y" (yes, use the cell).

    A reboot for reconfig permits the cell to rendezvous into the nPartition and become active; see below.
  - When you want to allow a currently inactive cell to become active.

    A reboot for reconfig reboots all cells, allowing them an opportunity to join (rendezvous) the nPartition as active members.

- Reset an nPartition to the ready for reconfig state (`shutdown -R -H`) to make the nPartition inactive.

  All cells in an nPartition remain inactive when the nPartition is in the ready for reconfig state; the cells do not perform a partition rendezvous.

- Perform a standard reboot (`shutdown -r`) of an nPartition in most other situations where you do not need to add or remove cells from the nPartition.

  A standard reboot causes only the *currently active* cells in an nPartition to reboot, and it does not allow any pending complex configuration changes to complete (the changes remain pending, still requiring a reboot for reconfig for them to be in effect).

  Pending changes that require a reboot for reconfig (`shutdown -R`, not a `shutdown -r`) include removing an active cell from an nPartition. The cell cannot be unassigned until its nPartition has a reboot for reconfig performed.

  Other changes, such as adding a cell to an nPartition or changing a cell's use-on-next-boot value from "n" to "y", also require performing a reboot for reconfig (`shutdown -R`, nor `-r`) to enable the inactive cell to become active.

5548

Listing the Local (Current) Partition Number

Each nPartition within a server complex has a unique number assigned to it. This **partition number** identifies the nPartition in various menus, commands, and utilities. You also can specify the partition number when performing operations on an nPartition, such as adding or removing cells or resetting an nPartition.

You can list the local partition number by using the following procedures:

- *Listing the Local nPartition Number [BCH]* on page 248
- *Listing the Local nPartition Number [HP-UX]* on page 248

Listing the Local nPartition Number [BCH]

Use the Configuration menu **PD** command to list the local partition number from the BCH interface.

Step 1. Access the Boot Console Handler (BCH) interface for the nPartition, and access the BCH Configuration menu.

Enter `CO` from the BCH Main menu to access the Configuration menu. If you are at a BCH menu other than the Main menu, enter `MA` to access the Main menu.

Step 2. From the BCH Configuration menu, enter the **PD** command to list the local nPartition's name and partition number.

```
Configuration Menu: Enter command > PD

Partition Number: 1
Partition Name: jules01

Configuration Menu: Enter command >
```

Listing the Local nPartition Number [HP-UX]

Use the **parstatus -w** command to list the partition number of the local (current) nPartition from HP-UX.

Step 1. Login to HP-UX running on the nPartition.

5547

Step 2. Issue the **parstatus -w** command to list the partition number for the local nPartition.

```
# parstatus -w
The local partition number is 0.
#
```

The parstatus -P command lists all nPartitions within the server complex, including the local nPartition.

```
# parstatus -P
[Partition]
Par                 # of  # of I/O
Num Status          Cells Chassis  Core cell  Partition Name (first 30 chars)
=== ============ ===== ======== ========== ==============================
 0  active          2      2      cab0,cell0 jules00
 1  active          2      2      cab0,cell4 jules01
#
```

Listing All Configured nPartitions

You can configure each server complex to have multiple nPartitions, which are composed of cells in the complex.

You can list all configured nPartitions in the server complex by using the following procedures:

- *Listing All nPartitions [Service Processor]* on page 250
- *Listing All nPartitions [HP-UX]* on page 251
- *Listing All nPartitions [Partition Manager]* on page 252

Listing All nPartitions [Service Processor]

Use the Command menu **CP** command to list all nPartitions in a server complex from the complex's service processor.

Step 1. Login to the service processor for the complex and enter **CM** to access the Command menu.

```
# telnet sdome-s
Trying...
Connected to sdome-s.rsn.hp.com.
Escape character is '^]'.
Local flow control off

GSP login: Accountname
GSP password: Password

....

GSP> CM
                Enter HE to get a list of available commands
GSP:CM>
```

Step 2. From the service processor Command menu, enter the **CP** command to list all configured nPartitions within the server complex.

The CP command lists each nPartition (by partition number) and indicates which cells from each cabinet are assigned to the nPartition.

In the following example the complex has two nPartitions: partition number 0 has cells 0 and 2, and partition number 1 has cells 4 and 6.

```
GSP:CM> CP

-------------------------------------------------------------------------------
Cabinet |    0    |    1    |    2    |    3    |    4    |    5    |    6    |    7
--------+---------+---------+---------+---------+---------+---------+---------+--------
 Slot   |01234567|01234567|01234567|01234567|01234567|01234567|01234567|01234567
--------+---------+---------+---------+---------+---------+---------+---------+--------
Part  0 |X.X.....|........|........|........|........|........|........|........
Part  1 |....X.X.|........|........|........|........|........|........|........

GSP:CM>
```

To the right of each partition number is a list of cells assigned to the nPartition. Assigned cells are marked with an "X". The cell's slot (0 to 7) and its cabinet number (0 or above) are listed above each cell.

You also can use the **DU** command to list *all* cells in a server complex (and other complex hardware details), including unassigned cells.

Listing All nPartitions [HP-UX]

Use the **parstatus -P** command (and **parstatus -C**, for more details) to list information about all nPartitions in a server complex from HP-UX.

From any nPartition in a complex, you can list details about all cells and nPartitions within the complex.

Step 1. Login to HP-UX running on any of the server complex's nPartitions.

You can login to HP-UX on the nPartition either by connecting with `telnet` or `rlogin`, or by logging in to its complex's service processor and accessing the nPartition's console.

Step 2. Issue the **parstatus -P** command to list brief details about all nPartitions in the server complex.

The `parstatus -P` command lists all nPartitions and shows each nPartition's number and name, the number of cells assigned to it, the number of active I/O chassis, and the nPartition's active core cell.

```
# parstatus -P
[Partition]
Par                # of  # of I/O
Num Status         Cells Chassis  Core cell  Partition Name (first 30 chars)
=== ============ ===== ======== ========== ==============================
```

SS44

```
 0  active          2      2      cab0,cell0 jules00
 1  active          2      2      cab0,cell4 jules01
#
```

While an nPartition is booting, the parstatus command cannot determine the nPartition's I/O chassis and core cell information. When this is the case parstatus does not count the I/O chassis and reports a question mark (?) for the core cell. When the nPartition has completed booting, parstatus reports all details.

Step 3. To list detailed information about all cells and nPartitions in the server complex, issue the **parstatus -C** command.

The parstatus -C command presents more detailed information about all cells and nPartitions. These details include each cell's status (active, inactive), its processor and memory configuration, its I/O chassis connections (if any), the cell's use-on-next-boot setting, and nPartition assignment.

```
# parstatus -C
[Cell]
                               CPU     Memory                                     Use
                               OK/     (GB)                               Core    On
Hardware   Actual              Deconf/ OK/                                Cell    Next Par
Location   Usage               Max     Deconf     Connected To            Capable Boot Num
========== ============ ======= ========= =================== ======= ==== ===
cab0,cell0 active core  4/0/4    2.0/ 0.0 cab0,bay0,chassis1  yes     yes  0
cab0,cell1 absent       -       -         -                   -       -    -
cab0,cell2 active base  4/0/4    2.0/ 0.0 cab0,bay1,chassis3  yes     yes  0
cab0,cell3 absent       -       -         -                   -       -    -
cab0,cell4 active core  4/0/4    2.0/ 0.0 cab0,bay0,chassis3  yes     yes  1
cab0,cell5 absent       -       -         -                   -       -    -
cab0,cell6 active base  4/0/4    2.0/ 0.0 cab0,bay1,chassis1  no      yes  1
cab0,cell7 absent       -       -         -                   -       -    -

#
```

For cells and nPartitions that have not finished booting, the parstatus command cannot determine processor, memory, or I/O details and instead reports a question mark (?) for these details.

Listing All nPartitions [Partition Manager]

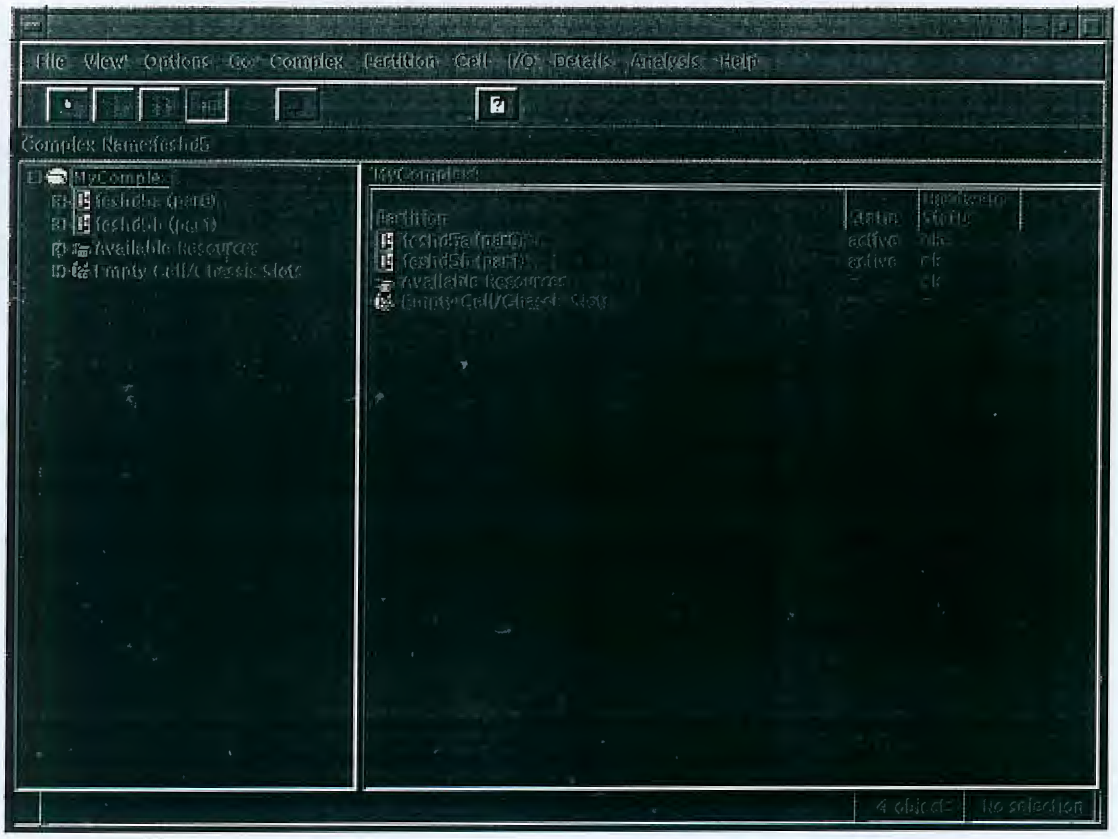
View the left side of Partition Manager primary window to see a list of all nPartitions in a server complex using Partition Manager.

Step 1. Run Partition Manager (/opt/parmgr/bin/parmgr) or access it from SAM or a Web browser.

me

SS43
21

Step 2. When the Partition Manager starts up, the left side of its primary display lists the nPartitions in the complex.



Partition	State	Hardware Status
feshd5a (par0)	active	ok
feshd5b (par1)	active	ok
Available Resources	-	ok
Empty Cell/Chassis Slots	-	-

The right side of the primary display also lists the complex's nPartitions when nothing is selected on the display's left side, or when **My Complex** is selected.

Listing Cell nPartition Assignments

Each cell in an nPartition server complex either is assigned to an nPartition, or it is unassigned (if it is an available resource).

You can list all cells and their nPartition assignments by using these procedures:

- *Listing Cell nPartition Assignments [Service Processor]* on page 254
- *Listing Cell nPartition Assignments [HP-UX]* on page 254
- *Listing Cell nPartition Assignments [Partition Manager]* on page 255

Listing Cell nPartition Assignments [Service Processor]

Use the Command menu's `CP` and `DU` commands to list all cell nPartition assignments (and other details) from the server complex's service processor.

Step 1. Login to the service processor for the complex and enter `CM` to access the Command menu.

Step 2. Enter the `CP` command to list all configured nPartitions in the server complex.

Step 3. Enter the `DU` command to list additional details (such as available core I/O) for the cells assigned to the various nPartitions in the server complex.

On HP Superdome servers, you also can use the service processor Command menu's `IO` command to list cell-to-I/O chassis connections.

Listing Cell nPartition Assignments [HP-UX]

Use the `parstatus -C` command to list all cells in a server complex and their nPartition assignments.

Step 1. Login to HP-UX running on one of the server complex's nPartitions.

Step 2. Issue the `parstatus -C` command to list all cells, any I/O chassis connections, and any nPartition assignments for the cells.

In addition to reporting the cell nPartition assignments (listed in the "Par Num" column), the parstatus -C command reports each cell's current status (absent, inactive, active core, active base) in the "Actual Usage" column.

```
# parstatus -C
[Cell]
                        CPU     Memory                              Use
                        OK/     (GB)                         Core   On
Hardware   Actual       Deconf/ OK/                          Cell   Next Par
Location   Usage        Max     Deconf    Connected To       Capable Boot Num
========== ============ ======= ========= =================== ======= ==== ===
cab0,cell0 active core  4/0/4    2.0/ 0.0 cab0,bay0,chassis1  yes     yes  0
cab0,cell1 absent       -       -         -                   -       -    -
cab0,cell2 active base  4/0/4    2.0/ 0.0 cab0,bay1,chassis3  yes     yes  0
cab0,cell3 absent       -       -         -                   -       -    -
cab0,cell4 active core  4/0/4    2.0/ 0.0 cab0,bay0,chassis3  yes     yes  1
cab0,cell5 absent       -       -         -                   -       -    -
cab0,cell6 inactive     4/0/4    2.0/ 0.0 cab0,bay1,chassis1  no      -    -
cab0,cell7 absent       -       -         -                   -       -    -

#
```

For cells that are not assigned to an nPartition, parstatus -C lists a hyphen (-) in the "Par Num" column instead of the cell's partition number. The "Connected To" column lists any I/O chassis connections for the cells, and "Core Cell Capable" lists whether core I/O is available through each the cell's I/O chassis.

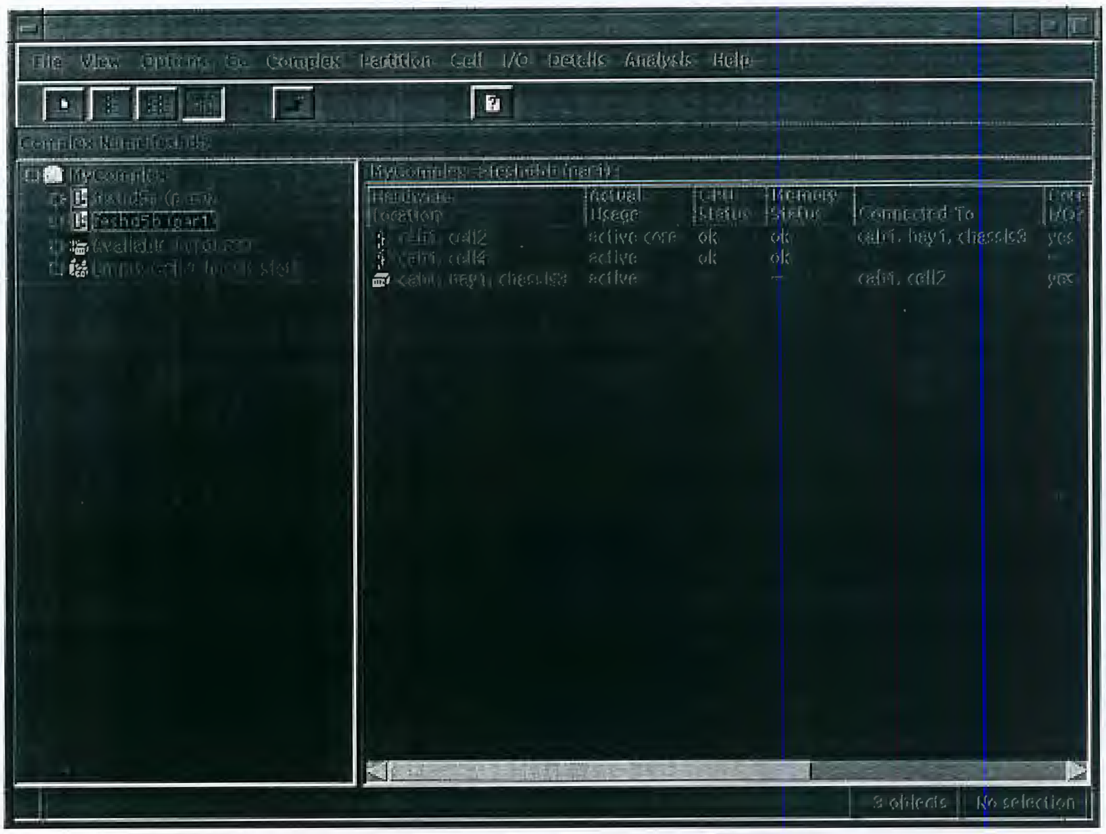
Listing Cell nPartition Assignments [Partition Manager]

Select each nPartition and Available Resources on the left side of the primary window to view all cell nPartition assignments in a server complex from Partition Manager.

Step 1. Run Partition Manager (/opt/parmgr/bin/parmgr) or access it from SAM or a Web browser.

Step 2. At the Partition Manager primary window, select each nPartition on the left side of the window to list the nPartition's cell assignments on the window's right side, or select Available Resources to list all unassigned cells.

5540



MyComplex->feshd5b (par1)

Hardware Location	Actual Usage	CPU Status	Memory Status	Connected To	Core I/O?
cab0, cell2	active core	ok	ok	cab0, bay1, chassis3	yes
cab0, cell4	active	ok	ok		–
cab0, bay1, chassis3	active		–	cab0, cell2	yes

3 objects | No selection

On the right side of the primary window, for each selected nPartition, Partition Manager lists the cell assignments and any I/O chassis connected to the cells.

5539

Creating a Genesis Partition

When you create a Genesis Partition, you establish a one-cell nPartition on the server complex. The Genesis Partition replaces all other nPartitions, and once created it is the only nPartition in the server.

The only way to create a Genesis Partition is to use the service processor Command menu's `CC` command on the server complex.

Genesis Partition Creation [Service Processor]

Use the service processor Command menu's `CC` command and `G` option to create a Genesis Partition on an HP nPartition server.

As a result of this procedure, *all existing nPartitions are destroyed* and are replaced with a single, one-cell nPartition (the Genesis Partition).

You can revert to the previous nPartition configuration—if any existed before you created the Genesis Partition—by using the `CC` command's `L` option to restore the last configuration.

Step 1. Save all current nPartition configuration details, if any nPartitions are configured in the complex.

Saving the current nPartition information provides you the details you would need to re-create all nPartitions as they currently exist.

Use the `parstatus -V -p#` HP-UX command (or an equivalent `parmgr` procedure) to save configuration details about each nPartition.

For each nPartition, enter the `parstatus -V -p#` command to display detailed information about the partition number (`-p#`) specified.

Step 2. Determine which cell will be configured as the Genesis Partition.

The cell must be connected to an I/O chassis. The I/O chassis must have a core I/O card installed, and it should have a bootable HP-UX disk (or a method for installing HP-UX and a disk onto which it can be installed).

Step 3. Ensure that all nPartitions within the complex are in the ready for reconfig (inactive) state.

538

If an nPartition is running HP-UX, you can shut down the nPartition to the ready for reconfig state by using the `shutdown -R -H` command.

Or, you can put an nPartition into the ready for reconfig state by using the BCH interface's `RECONFIGRESET` command or using the service processor Command menu's `RR` command.

Step 4. Login to the server complex's service processor (GSP or MP).

Login as a user with administrator privileges, which are required for creating a Genesis Partition.

Step 5. Enter **`CM`** to access the service processor Command menu.

Step 6. Issue the **`CC`** command, select **`G`** for Genesis Complex Profile, and specify the cabinet and cell slot for the cell that will comprise the Genesis Partition.

```
GSP:CM> CC


This command allows you to change the complex profile.

WARNING: You must shut down all Protection Domains before
executing
         this command.


G - Genesis Complex Profile
L - Last Complex Profile
    Select Profile: g

    Enter Cabinet number: 0

    Enter Slot number: 0

    Do you want to modify the complex profile? (Y/[N]) y

    -> The complex profile will be modified.
GSP:CM>
```

You can confirm that the Genesis Partition was successfully created if the `CC` command reports that the “complex profile will be modified”.

If the `CC` command reports “Sorry, command failed”, then the Genesis Partition was not created, possibly because one or more nPartitions are not at the ready for reconfig state. If this is the case, go back to *Step 3* and ensure all nPartitions are inactive at the ready for reconfig state.

5537

Step 7. Issue the BO command to boot the Genesis Partition past its ready for reconfig state and make it an active nPartition.

When a Genesis Partition is created, it remains at boot-is-blocked (in an inactive, ready for reconfig state), so you must boot it manually.

The Genesis Partition always is assigned partition number 0, because when it is created it is the first and only nPartition in the server complex.

Using the BO command to boot partition 0 will boot the Genesis Partition to its Boot Console Handler (BCH) interface.

```
GSP:CM> BO

This command boots the selected partition.

     #    Name
    ---   ----
     0)   Partition 0

    Select a partition number : 0

    Do you want to boot partition number 0,
    named Partition 0 ? (Y/[N]) y

    -> The selected partition will be booted.
GSP:CM>
```

Step 8. Access the Genesis Partition's console and configure the nPartition as appropriate and necessary.

From the service processor Command menu, enter **MA** to return to the Main menu, then enter **CO** to access the Console menu. The Genesis Partition is partition 0 and by default is named "Partition 0".

You will need to set the boot paths (PRI, ALT, and HAA), any core cell choices, the nPartition name, and other settings as appropriate. You also may need to add cells to the Genesis Partition if you want it to have more than one cell.

5536

Creating a New nPartition

In a server complex, you can create multiple nPartitions if the server has enough cells and core I/O to support the nPartitions.

You can create a new nPartition by using the following procedures:

- *Creating a New nPartition [HP-UX]* on page 260
- *Creating a New nPartition [Partition Manager]* on page 264

At least one cell in each nPartition must be connected to an I/O chassis that has core I/O attached. To boot HP-UX the nPartition also must have a boot device and any required PCI cards and devices installed.

When creating an nPartition, you should adhere to the HP nPartition requirements and guidelines. HP recommends only specific sets of nPartition configurations.

If no nPartitions exist in a server complex, you must first establish a Genesis Partition before creating other nPartitions.

Creating a New nPartition [HP-UX]

Use the **parstatus**, **parcreate**, and **parmodify** commands to create and configures a new nPartition from HP-UX.

This procedure uses parstatus to find available (unassigned) cells, uses parcreate to create an nPartition using the cells, and uses parmodify to modify the nPartition's settings and configure it for use.

One alternative to using this complete procedure is to replace steps 2–5 with a single parcreate command.

For example, the commands performed in steps 2–5 could be replaced with the following parcreate command line.

```
# parcreate -c4:base:y:ri -c6:base:y:ri -P "hostname05" -r0/4 \
> -r0/6 -b 4/0/1/0/0.9 -B
Partition Created. The partition number is : 1
#
```

5535
21

In the above alternative command line, the -B option is specified and causes the nPartition to be booted past boot-is-blocked immediately, thus making the new nPartition active. (It is booted to its BCH interface.)

Step 1. Login to HP-UX running on an existing nPartition in the server complex, and plan your nPartition configuration by selecting which cells will comprise the new nPartition.

Use the **parstatus -AC** command to list all unassigned (available) cells in the server complex.

```
# parstatus -AC
[Cell]
                        CPU     Memory                                Use
                        OK/     (GB)                          Core    On
Hardware   Actual       Failed/ OK/                           cell    Next Par
Location   Usage        Max     Failed  Connected To          Capable Boot Num
========== ============ ======= ======= ===================== ======= ==== ===
cab0,cell1 absent       -       -       -                     -       -    -
cab0,cell3 absent       -       -       -                     -       -    -
cab0,cell4 power on     4/0/4   2.0/0.0 cab 0,bay0,chassis3 yes     -    -
cab0,cell5 absent       -       -       -                     -       -    -
cab0,cell6 power on     4/0/4   2.0/0.0 cab 0,bay1,chassis1 yes     -    -
cab0,cell7 absent       -       -       -                     -       -    -

#
```

You can select any of the cells listed to create the new nPartition; only the cells that are *not "absent"* are present within the server complex.

All cells that you choose **must** meet the hardware requirements for nPartitions (for example, they all must have the same processor revision and firmware) and **should** form an HP-recommended nPartition configuration. At least one cell must have an I/O chassis with core I/O.

Step 2. After confirming that cells you have chosen would establish a valid nPartition configuration, use the **parcreate -c**... command to create a new nPartition with the cells.

When using the parcreate command, *do not* specify the -B option for this procedure.

(The -B option causes parcreate to immediately boot the newly-created nPartition past the default ready for reconfig state, thus making the nPartition active and preventing you from further modifying it.)

5530

By *not* specifying `-B`, the new nPartition can be further modified because it will remain inactive at the ready for reconfig state (until you boot it using the service processor Command menu's `BO` command).

If creating a single-cell nPartition, just use one `-c` option.

To create a multiple-cell nPartition, you should specify the `-c` option multiple times (once for each cell) issuing a single command line.

```
# parcreate -c4:base:y:ri -c6:base:y:ri
Partition Created. The partition number is : 1
#
```

When `parcreate` successfully creates a new nPartition, it reports "Partition Created" and reports the nPartition number ("partition number is...").

If parcreate detects any problems or issues when creating an nPartition, it lists them in its output. If it cannot create the nPartition, `parcreate` reports "Command failed" along with more details.

The `parcreate` command's `-c` option is as follows:

`-c` *`cell`*`:`[*`cell_type`*]`:`[*`use_on_next_boot`*]`:`[*`failure_usage`*]

This option specifies the cell ID (*`cell`*) to be assigned to the nPartition.

- The only valid *`cell_type`* value is: `base` (base cell, the default).
- The valid *`use_on_next_boot`* values for cells are:

  `y` Participate in reboot (the default).

  `n` Do not participate in reboot.
- The only valid *`failure_usage`* value is: `ri` (reactivate with interleave, the default).

For details, see the *parcreate* (1M) manpage.

Step 3. Use the **`parmodify`** command to modify the new nPartition's configuration and set the nPartition name (`-P`), boot paths (`-b`, `-s`, and `-t`), and any core cell choices (`-r`).

When using the `parmodify` command, you must use the `-p#` option to specify the partition number for the nPartition. Use the partition number that the `parcreate` command reported in *Step 2*.

5533

```
# parmodify -p1 -P "hostname05"
Command succeeded.
# parmodify -p1 -r0/4 -r0/6
Command succeeded.
# parmodify -p1 -b 4/0/1/0/0.9
Command succeeded.
#
```

When each modification takes place, parmodify reports "Command succeeded". Otherwise it reports any problems.

You can specify each configuration option on a separate command line or can combine all options into a single, longer command line.

For details on the various options for modifying nPartition settings, see the *parmodify* (1M) manpage.

Step 4. Use the **parstatus -V -p#** command to list all details about your newly created and configured nPartition.

If any configuration details should be modified, use the parmodify command before you boot the nPartition in the next step.

```
# parstatus -V -p1
[Partition]
Partition Number        :  1
Partition Name          : hostname05
Status                  : inactive
IP address              :
Prmary Boot Path        : 4/0/1/0/0.9
ALternate Boot Path     : 0/0/0/0/0/0/0/0.0.0
HA Alternate Boot Path  : 0/0/0/0/0/0/0/0.0.0
PDC Revision            : 104.1
IODCH Version           : 23664
CPU Speed               : 552 MHz
Core Cell               : ?
Core Cell Alternate     :
                0. cab0,cell4
                1. cab0,cell6
[Cell]
                        CPU     Memory                             Use
                        OK/     (GB)                       Core    On
Hardware   Actual       Failed/ OK/                        cell    Next Par
Location   Usage        Max     Failed    Connected To     Capable Boot Num
========== ============ ======= ========= ================= ======= ==== ===
cab0,cell4 inactive     4/0/4    2.0/ 0.0 cab 0,bay0,chassis3 yes     yes  1
cab0,cell6 inactive     4/0/4    2.0/ 0.0 cab 0,bay1,chassis1 yes     yes  1
....
```

5332

Step 5. Boot your newly-created nPartition past boot-is-blocked to make it active and make its BCH interface available.

Use the service processor Command menu's BO command to boot the nPartition.

Once the nPartition is booted, you can access its BCH interface through its console. Use the service processor Console menu (enter CO at the service processor Main menu).

Creating a New nPartition [Partition Manager]

Use the **Partition —> Create Partition** action to create a new nPartition using Partition Manager.

Step 1. Plan your nPartition configuration by selecting which cells will comprise the new nPartition.

All cells that you choose **must** meet the hardware requirements for nPartitions (for example, they all must have the same processor revision and firmware) and **should** form an HP-recommended nPartition configuration. At least one cell must have an I/O chassis with core I/O.

Step 2. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

You optionally can specify the `parmgr -t create` command and options to automatically launch the **Partition —> Create Partition** action. See the *parmgr* (1M) manpage for command option details.

Step 3. Select the **Partition —> Create Partition** action to run the Partition Manager task wizard for creating a new nPartition.

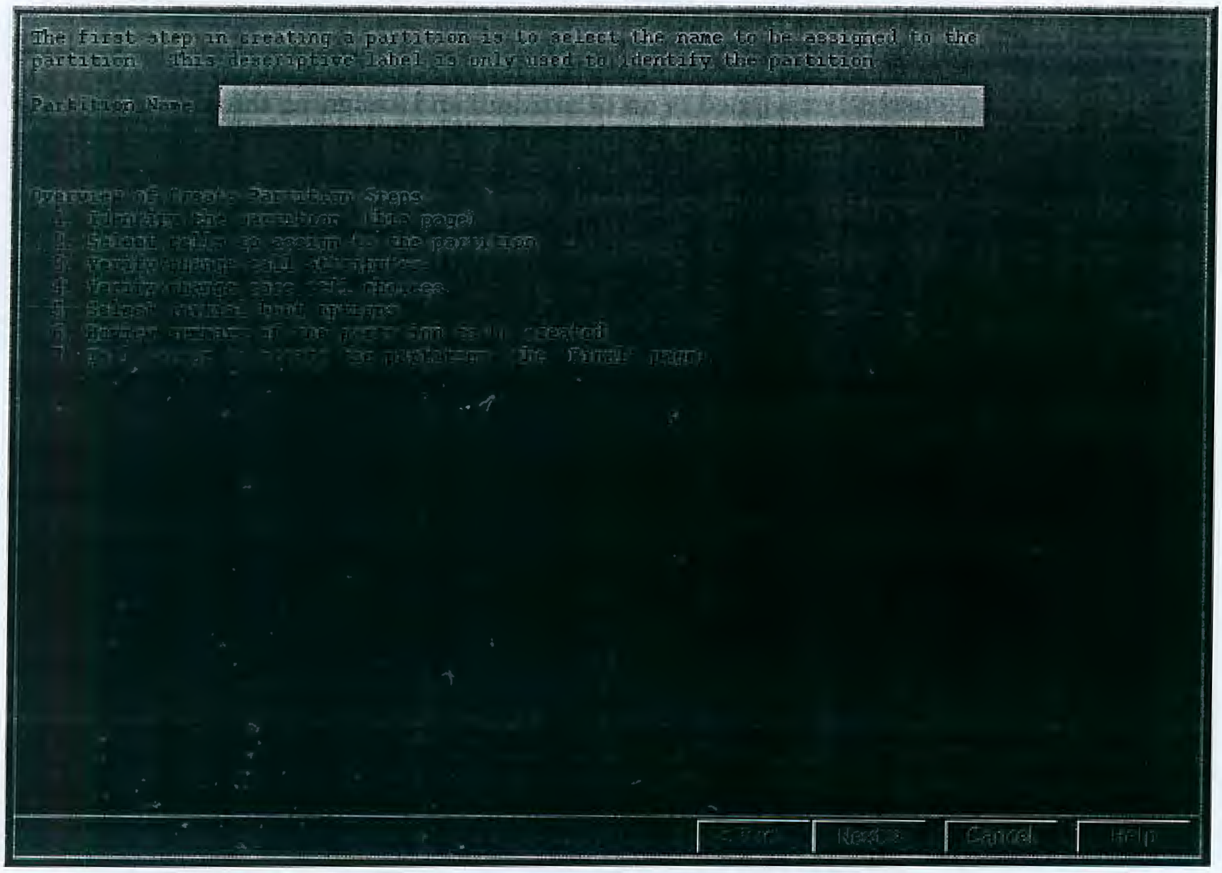
Partition Manager guides you through the steps it requires for creating a new nPartition.

You can move backward and forward through the steps by using **Next** and **Back** buttons. At the final steps, you can verify the settings you have established for the new nPartition and, if they are correct for your purposes, click the **Finish** button to create the new nPartition.

You can *cancel the new nPartition* creation at any time by clicking the **Cancel** button.

5531

The following window shows the first step and overview for Partition Manager's create **Partition —> Create Partition** action.



The first step in creating a partition is to select the name to be assigned to the partition. This descriptive label is only used to identify the partition.

Partition Name:

Overview of Create Partition Steps
1. Identify the partition (this page)
2. Select cells to assign to the partition
3. Verify/change cell attributes
4. Verify/change core cell choices
5. Select optional boot options
6. Review summary of the partition to be created
7. Finish and create the partition (the Finish page)

If you specify for Partition Manager to automatically boot the new nPartition, you can access the new nPartition's BCH interface from its console when you finish using the create partition task wizard.

Otherwise, if you *do not* specify to automatically boot the new nPartition, you must use the service processor Command menu's BO command to boot the nPartition past boot-is-blocked (inactive, ready for reconfig state) and make its BCH interface available.

SS30

Assigning (Adding) Cells to an nPartition

You can add cells to the local nPartition or to any remote nPartitions in the same server complex.

Adding cells to an nPartition involves selecting available cells (those not currently assigned to an nPartition) and assigning them to an existing nPartition. Both the selected cells and any I/O chassis connected to the cells are assigned to the designated nPartition.

You can add cells to an nPartition by using the following procedures:

- *Adding Cells to an nPartition [HP-UX]* on page 267
- *Adding Cells to an nPartition [Partition Manager]* on page 268

When adding cells to an nPartition, you should refer to the guidelines in the chapter *Planning nPartition Configurations* on page 109.

Reboot for Reconfig Guidelines for Adding Cells

In some situations, you must immediately perform a reboot for reconfig of a modified nPartition after adding cells to it.

- You **must** immediately perform a reboot for reconfig (`shutdown -R`) of an nPartition when you have added a cell to an active nPartition and you specified the `-B` option to the `parmodify` command.
- You **should** perform a reboot for reconfig of an nPartition *as soon as possible* after you have added a cell to an active nPartition and have specified a "y" use-on-next-boot value for the new cell.
- You need not perform a reboot for reconfig of an nPartition in these situations:
  - When you have added a cell to an inactive nPartition.
  - When you have added a cell with a "n" use-on-next-boot value and you did not specify the `-B` option to the `parmodify` command.

Adding Cells to an nPartition [HP-UX]

Use the `parstatus` and `parmodify` commands to add cells to an nPartition using HP-UX commands.

Step 1. Use the `parstatus -A -C` command to list all available cells (the unassigned cells) in the server complex.

Step 2. Choose one or more eligible cells from the list to add to the nPartition.

Adding the cell(s) to the nPartition should create a configuration that adheres to the hardware requirements and performance guidelines.

Step 3. Modify the nPartition by issuing the `parmodify -p# -a#...` command to add the cell.

The `-p#` option specifies the partition number (#) for the nPartition being modified.

The `-a` *`cell:type:use:fail`* option specifies the cell ID and other details for the cell to be added to the nPartition.

To add multiple cells, you can specify the `-a` option multiple times in the same command.

For example: `parmodify -p1 -a0:base:y:ri -a2:base:y:ri` adds two cells (cell ID 0 and cell ID 2) to nPartition number 1.

The `-a` option (`-a` *`cell:type:use:fail`*) specifies the following details for each cell that you add to the nPartition.

`cell` The cell to be added to the nPartition. You can specify the cell in global (*`cell`*) format or in hardware location (*`cabinet/slot`*) format.

`type` The cell type: `base` is the only supported cell type and it is the default.

`use` The cell's use-on-next-boot value: `y` or `n`. Use `y` (the default) if the cell is to be an active member of the nPartition, or use `n` if the cell is to remain an inactive member.

`fail` The cell's failure usage: `ri` (reactivate with interleave) is the only supported failure usage policy and it is the default.

SS28

You can optionally specify the `parmodify` command's `-B` option to require that the modified nPartition be rebooted.

- When you specify `-B` to modify an *inactive* nPartition, the inactive nPartition completes partition rendezvous and becomes active if possible.
- When you specify `-B` to modify an *active* nPartition, you must perform a reboot for reconfig of the nPartition before any other cell assignment changes can be made within the server complex.

The `parmodify -p1 -a0:base:y:ri -a2:base:y:ri` command adds cell 0 and cell 2 to partition number 1. This command also sets a "y" use-on-next-boot value for both cells, meaning that they will be active members of the nPartition following the next time all cells boot (for example, when reboot for reconfig is performed on the nPartition.

Because this example command does not include the `-B` option, if partition 1 were an *inactive nPartition*, it would remain inactive; if partition 1 were an *active nPartition* the new cells would be assigned, but they would remain inactive cells until a reboot for reconfig is performed.

See the *parmodify* (1M) manpage for details on all options.

Step 4. As needed, perform a reboot for reconfig (**`shutdown -R`**) on the modified nPartition.

See the *Reboot for Reconfig Guidelines for Adding Cells* on page 266 for details on when to perform a reboot for reconfig.

Adding Cells to an nPartition [Partition Manager]

Use the **Partition —> Modify Partition** action, **Add/Remove Cells** tab to add cells to an nPartition from Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. In the Partition Manager primary window, select the nPartition to which you want to add cells, then select the **Partition —> Modify Partition** menu item.

Step 3. In the Modify Partition window, click the **Add/Remove Cells** tab.

Step 4. Select the cells that you want to add to the nPartition from the Available Cells list, then click the **Add** button to add them to the nPartition's cell list.

If adding multiple cells, you can select multiple cells by pressing the **Control** key while clicking on the cells.

Adding the cell(s) to the nPartition should create a configuration that adheres to the hardware requirements and performance guidelines.

Step 5. After you add the new cells to the nPartition's cell list, click the **OK** button.

The cells are not actually *assigned* to the nPartition until after the next step.

Step 6. Review the information shown in the **Notes and Warnings**, the **Summary of Changes**, and the **HA Checks** tabs.

Partition Manager generates this information when it checks details of the new nPartition configuration, such as cell compatibility and various high-availability guidelines.

To cancel all nPartition changes, click the **Cancel** button in the Notes and Warnings window and then click **Cancel** in the Modify Partition window.

To proceed with adding the cell(s) to the nPartition, click **OK**.

Step 7. Once Partition Manager confirms that the "partition has been successfully modified" click the **OK** button.

The cells are assigned to the nPartition after clicking **OK** in the previous step. However, any cells you have added to an active nPartition will remain *inactive* until you perform a reboot for reconfig of the modified nPartition.

Step 8. As needed, perform a reboot for reconfig (`shutdown -R`) of the modified nPartition.

See the *Reboot for Reconfig Guidelines for Adding Cells* on page 266 for details on when to perform a reboot for reconfig.

5526

Unassigning (Removing) Cells from an nPartition

Removing a cell from an nPartition involves unassigning the cell from the nPartition to which it is assigned and, if necessary, performing a reboot for reconfig of the nPartition.

You can remove *any cell* from the local nPartition and can remove *inactive cells* from remote nPartitions in the same server complex. However, at least one core-capable cell must remain in each nPartition.

You can remove (unassign) cells from nPartitions by using these procedures:

- *Removing Cells from an nPartition [HP-UX]* on page 271
- *Removing Cells from an nPartition [Partition Manager]* on page 274

When removing cells from an nPartition, you should ensure that the modified nPartition still adheres to the hardware requirements and performance guidelines for nPartitions. Refer to the chapter *Planning nPartition Configurations* on page 109 for details.

After you remove a cell from an nPartition, the cell's I/O chassis also is removed from the nPartition. As a result, any I/O devices associated with the cell are made unavailable to the nPartition after the cell is removed.

If you want to remove the last cell in an nPartition, you must instead remove the nPartition using the `parremove` command or Partition Manager.

Once a cell is unassigned, the cell (and any I/O resources connected to the cell) is considered to be an available resource that is on the "free cell list" and can be assigned to any nPartition in the server complex.

Reboot for Reconfig Guidelines for Removing Cells

In some situations, you must immediately perform a reboot for reconfig (`shutdown -R`) of a modified nPartition after removing cells from it. Performing a required reboot for reconfig completes cell assignment changes and unlocks the server's Complex Profile.

- You **must** immediately perform a reboot for reconfig of an nPartition when you have removed an *active cell* from the nPartition.
- You **must** immediately perform a reboot for reconfig of an nPartition when you have removed a cell from an active nPartition and specified the `-B` option to the `parmodify` command.
- You need not perform a reboot for reconfig of an nPartition when you have removed an *inactive* cell from an nPartition and did not specify the `-B` option to the `parmodify` command.

In the cases where you must immediately perform a reboot for reconfig after removing a cell, *not doing so* will leave the Complex Profile locked and thus will prevent any other changes to the server complex configuration. In these cases, the reboot for reconfig is required to complete the cell assignment changes and permit other changes to occur.

Removing Cells from an nPartition [HP-UX]

Use the **`parstatus`** and **`parmodify`** commands to remove cells from an nPartition using HP-UX commands.

Step 1. List the current nPartition assignments and status for the cells you plan to remove from their assigned nPartition by issuing the **`parstatus -c#...`** HP-UX command.

Specify each cell you plan to remove with a separate `-c` option.

For example, to list details on cells 0, 1, and 2, issue the `parstatus -c0 -c1 -c2` command.

The cells must all be assigned to the same nPartition in order to remove them using a single procedure. Otherwise, if the cells are assigned to different nPartitions, you must perform this procedure separately for each nPartition.

SS24

In order to remove cells that are not assigned to the local nPartition, the cells must be *inactive* (their “Actual Usage” must be “inactive”). You can list the local nPartition by issuing the `parstatus -w` command.

To remove an *active* cell from its nPartition, you must do so when logged in to HP-UX running on the cell’s nPartition.

Step 2. Remove the cell from the nPartition to which it is assigned by using the **`parmodify -p# -d#...`** command.

Specify the partition number (`-p#`) and each cell (`-d#`) that you want to remove from the nPartition.

If removing *multiple cells* from an nPartition, specify each cell with a separate `-d#` option on the same command line (such as: `parmodify -p1 -d0 -d2...` to remove cells 0 and 2 from partition number 1).

Slightly different procedures are required for removing active cells and inactive cells. See the following information for details (*Guidelines for Removing an Active Cell* and *Guidelines for Removing an Inactive Cell*).

When you are removing multiple cells from the local nPartition, if at least one of the cells you plan to remove is currently active, then you should follow the guidelines for removing active cells.

- **Guidelines for Removing an Active Cell**

  You **should** specify the `-B` option to `parmodify` when removing an active cell from the local nPartition if you want the nPartition to become active following its reboot for reconfig.

  For example, the following command removes cell 4 from partition 0 and the `-B` option ensures that the nPartition will be active following its reboot for reconfig.

  ```
  # parmodify -p0 -d4 -B
  Cell 4 is active.
  Use shutdown -R to shutdown the system to ready for
  reconfig state.
  Command succeeded.
  #
  ```

  You **must** perform a reboot for reconfig (`shutdown -R`) after you issue the `parmodify` command to remove active cell(s) from the nPartition. (This is covered in *Step 3* that follows.)

- **Guidelines for Removing an Inactive Cell**

  When removing an *inactive* cell from an nPartition you do not need to specify the `-B` option to `parmodify` and do not need to perform a reboot for reconfig of the cell's nPartition.

  When you use `parmodify` to remove an inactive cell, the cell is immediately unassigned from its nPartition.

  If you specify the `-B` option when removing an *inactive cell* from an *inactive nPartition*, then the cell is immediately removed and the modified nPartition is booted past its inactive ready for reconfig state and becomes an active nPartition.

  For example, the following command removes cell 2 from partition 0. Because cell 2 is inactive, it is immediately unassigned.

  ```
  # parmodify -p0 -d2
  Command succeeded.
  #
  ```

Step 3. As needed, perform a reboot for reconfig (**`shutdown -R`**) of the nPartition being modified.

You **must** perform a reboot for reconfig if you have removed an *active cell* or have specified the `-B` option when modifying an *active nPartition*.

See the *Reboot for Reconfig Guidelines for Removing Cells* on page 271 for details on when to perform a reboot for reconfig.

This reboot for reconfig enables the cell removal to complete and the Complex Profile to be unlocked.

If you have removed an active cell and you did not specify the `-B` option to `parmodify`, then the nPartition will remain *inactive* in the ready for reconfig state after you perform the reboot for reconfig. To make the inactive nPartition active, use the service processor Command menu's `BO` (boot) command.

SS22

Removing Cells from an nPartition [Partition Manager]

Use the **Partition —> Modify Partition** action, **Add/Remove Cells** tab to remove cells from an nPartition using Partition Manager.

Step 1. Determine which cell(s) you want to remove from the nPartition.

The cells must all be assigned to the same nPartition in order to remove them using a single procedure. Otherwise, if the cells are assigned to different nPartitions, you must perform this procedure separately for each nPartition.

Step 2. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 3. In the Partition Manager primary window, select the nPartition from which you want to remove cells, then select the **Partition —> Modify Partition** action.

Step 4. In the Modify Partition window, click the **Add/Remove Cells** tab.

Step 5. From the "Cells in the Partition" list, select the cells that you want to remove from the nPartition. Then click the **Remove** button to move them to the Available Cells list. If removing multiple cells, you can select multiple cells by pressing the **Control** key while clicking on the cells.

Removing the cell(s) from the nPartition should create a configuration that adheres to the hardware requirements and performance guidelines.

Step 6. After you have removed the cells from the nPartition's cell list, click the **OK** button.

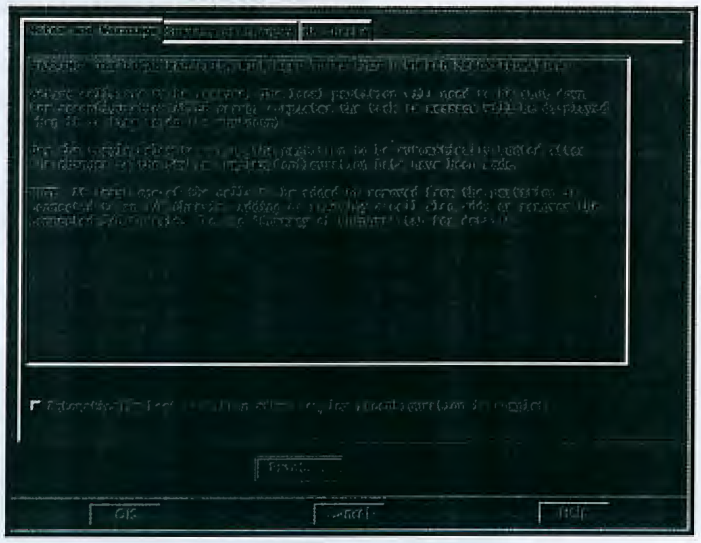
The cells are not actually *removed* from the nPartition until after the next step.

Step 7. Review the information shown in the **Notes and Warnings**, the **Summary of Changes**, and the **HA Checks** tabs.

Partition Manager generates this information when it checks details of the new nPartition configuration.

If you **must** perform a reboot for reconfig of the nPartition, such as when removing an active cell from the nPartition, then the Notes and Warnings tab provides details and options.

- If a reboot for reconfig is required, the Notes and Warnings tab has information about the reboot procedure. (See *Step 9* for details.)



- When a reboot for reconfig is required, the Notes and Warnings tab also has a check box ("Automatically boot partition") that—when selected—enables the nPartition to rendezvous and be active after the reboot for reconfig.

To cancel all nPartition changes, click the **Cancel** button in the Notes and Warnings window and then click **Cancel** in the Modify Partition window.

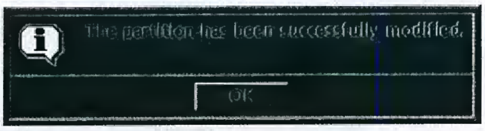
To proceed with removing the cell(s) from the nPartition, click **OK**.

Step 8. When Partition Manager confirms that the "partition has been successfully modified", review any additional information and respond as needed to the dialog box presented.

(The cells were designated to be removed from the nPartition after completing the previous step, however a reboot may be required.)

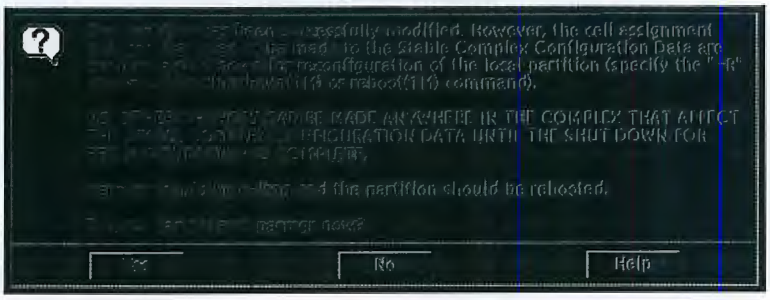
- If you have removed only *inactive* cells from the nPartition, Partition Manager provides no additional info and you can click **OK** to complete the procedure (a reboot is not needed).

SS20
22


The partition has been successfully modified.

- If you have removed one or more *active* cells from the nPartition, then Partition Manager provides more info about performing the required reboot for reconfig of the nPartition.

  You **must** reboot the nPartition as soon as possible, so you should click the **Yes** button to exit Partition Manager and proceed with the next step of this procedure.


[illegible] been successfully modified. However, the cell assignment [illegible] made to the Stable Complex Configuration Data are [illegible] for reconfiguration of the local partition (specify the "-R" [illegible] shutdown(1M) or reboot(1M) command).

[illegible] CAN BE MADE ANYWHERE IN THE COMPLEX THAT AFFECT [illegible] CONFIGURATION DATA UNTIL THE SHUT DOWN FOR [illegible] COMPLETE.

[illegible] and the partition should be rebooted.

[illegible] manager now?

Step 9. As needed, perform a reboot for reconfig (**`shutdown -R`**) of the modified nPartition.

- If you have removed only inactive cells from an nPartition, then you *do not* need to perform a reboot for reconfig of the nPartition.

- If you have removed any active cells from the nPartition, then you **must** perform a reboot for reconfig and will have seen a detailed message about rebooting from Partition Manager (see *Steps 7 and 8*).

  After you issue the `shutdown -R` command, the nPartition performs the reboot for reconfig. If you selected the "Automatically boot partition" check box earlier in this procedure (see *Step 7*), then the nPartition is active after the reboot for reconfig and you can interact with it through its console.

If you *did not* select the "Automatically boot partition" check box, then the nPartition is inactive (at the ready for reconfig state) after the reboot for reconfig occurs. In this situation, you can make the nPartition active by using the service processor Command menu's BO command.

SS18
20

Removing (Deleting) an nPartition

You can delete (remove) any nPartition within a server complex.

The HP-UX nPartition deletion capabilities include restrictions for security reasons: you can delete only the *local nPartition* and *inactive remote* nPartitions.

You can delete an nPartition using these procedures:

- *Deleting an nPartition [HP-UX]* on page 278
- *Deleting an nPartition [Partition Manager]* on page 280

When removing the local nPartition, you must complete the procedure by issuing the **`shutdown -R -H`** command *as soon as possible* after initiating the local nPartition's removal.

Deleting an nPartition causes all of the nPartition's cells (and any I/O resources connected to the cells) to be unassigned. As a result, all of these cells become available resources that are on the "free cell list" and can be assigned to any nPartition in the server complex.

Deleting an nPartition [HP-UX]

Use the **`parremove`** command to delete an nPartition using HP-UX commands.

Step 1. Use the **`parstatus -P`** command to list all nPartitions, and check the status (active or inactive) for the nPartition you plan to remove.

To check the *local* partition number, use the `parstatus -w` command. The local nPartition always is active when it is running HP-UX.

If you are planning to remove a *remote* nPartition, check to see whether the remote nPartition is inactive.

Step 2. If a remote nPartition that you plan to remove currently is *active*, then put the nPartition into the ready for reconfig state to make it inactive.

If the remote nPartition is running HP-UX, you can shut down the nPartition to the ready for reconfig state by 1) logging in to HP-UX on the remote nPartition, 2) shutting down all applications and warning users, and 3) issuing the `shutdown -R -H` command.

5517

You also can put the nPartition into the ready for reconfig state by using the BCH interface's `RECONFIGRESET` command or the service processor Command menu's `RR` command.

Step 3. Save all current configuration details about the nPartition you plan to remove.

Use the **`parstatus -V -p#`** command to display all current configuration information related to the nPartition you plan to remove.

Save this information, as you can use it to manually recreate the nPartition if necessary at a later time.

Step 4. Remove the nPartition.

Use one of the following procedures (*Removing an Inactive Remote nPartition* or *Removing the Local nPartition*) to remove the nPartition.

- **Removing an Inactive Remote nPartition**

  1. Issue the `parremove -p#` command to remove the inactive remote nPartition, where the `-p#` option specifies the partition number. For example:

     ```
     # parremove -p1
     ```

  2. Issue the `parstatus -P` command to confirm that the nPartition was removed.

     If the nPartition was removed, it no longer is listed in the `parstatus` command's output.

- **Removing the Local nPartition**

  To remove the local nPartition (the nPartition on which you currently are issuing commands), perform the following steps.

  1. Shut down all applications and warn users. Follow the same procedures you would use if you were to reboot the nPartition.

  2. Issue the `parremove -F -p#` command, which initiates the complex profile revisions that will take place when the nPartition is removed.

     When using `parremove` to remove the local nPartition, you must specify both the `-p#` option (to specify the local partition number) and the `-F` option (to force-remove the local nPartition).

SS16

28

Note that the local nPartition remains active following the `parremove -F -p#` command, until you perform a shutdown for reconfig (`shutdown -R -H`) to complete the removal.

As soon as possible you should proceed with the shutdown for reconfig because the server Complex Profile will remain locked—and no other changes can occur—until the pending nPartition removal is completed.

3. Perform a shutdown for reconfig (`shutdown -R -H`) of the local nPartition.

   The `shutdown -R -H` command shuts down the nPartition and all cells so that the configuration changes occur and the nPartition is deleted.

After you complete the nPartition removal, the nPartition no longer exists—its configuration information has been deleted.

All cells (and associated I/O chassis) that used to be assigned to the deleted nPartition now are unassigned and can be assigned for other uses.

Deleting an nPartition [Partition Manager]

Use the **Partition —> Delete Partition** action to remove an nPartition using Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. In the Partition Manager primary window, select the nPartition you want to remove.

Click the nPartition's name in the list on the left side of the primary window to select the nPartition.

If you plan to remove a *remote nPartition*, then after you select the nPartition's name, all of the nPartition's hardware (listed on the right side of the primary window) should be listed as having an Actual Usage of "inactive". To remove a remote nPartition it must be inactive.

NR

Step 3. Select the **Partition —> Delete Partition** action to request that the selected nPartition be removed (deleted).

Partition Manager presents the following window to confirm whether you want to delete the selected nPartition.

You can view details about the nPartition by clicking the **Show Details** button, or cancel the deletion by clicking **Cancel**.

Step 4. Proceed with the nPartition deletion by clicking the **OK** button in the Partition Manager confirmation window.

Step 5. Perform any remaining tasks (such as a `shutdown -R -H`) as needed.

You may need to perform a shutdown for reconfig, depending on the type of nPartition you are removing (local or remote) and its state (active or inactive). Review the following list for details:

- If you are removing a *remote* nPartition that was *inactive*, the nPartition was removed immediately so this removal procedure is finished and you do not need to perform any shutdowns.

- If you attempt to remove a *remote* nPartition that is *active*, Partition Manager cannot remove the remote nPartition. You first must make the remote nPartition inactive by putting it into the ready for reconfig state.

  To put the remote nPartition in the ready for reconfig state: login to the remote nPartition and issue the `shutdown -R -H` command, or issue the BCH `RECONFIGRESET` command or the service processor `RR` command for the remote nPartition.

  After the remote nPartition is inactive, you must perform this removal procedure again using Partition Manager on the local nPartition if you want to remove the remote nPartition.

- If you are removing the *local* nPartition, Partition Manager will display the following information to you after you click **OK** to remove the nPartition.

  To complete the local nPartition's removal, you must perform a shutdown for reconfig (`shutdown -R -H`) of the local nPartition as soon as possible.

5514

Because the Complex Profile will remain locked until the local nPartition's removal is completed, no other changes can occur in the server complex until you perform the shutdown for reconfig.

After Partition Manager removes an nPartition, the nPartition no longer exists—its configuration information has been deleted.

All cells (and associated I/O chassis) that used to be assigned to the deleted nPartition now are unassigned and are available resources that can be assigned for other uses.

5573
2l

Naming and Renaming nPartitions

Each nPartition has both a partition *number* and an nPartition *name*.

The **partition name** for each nPartition can have from 1 to 64 characters, including upper- and lowercase letters; numbers; and dashes, underscores, and spaces ("-" "_" and " ").

You can customize each nPartition's name to help you distinguish among the nPartition in a server complex. (You cannot change the partition number, which is a permanent unique identifier that is automatically assigned for each nPartition in a server complex.)

You can name and rename nPartitions using these procedures:

- *Renaming an nPartition [BCH]* on page 283
- *Renaming an nPartition [HP-UX]* on page 284
- *Renaming an nPartition [Partition Manager]* on page 285

Partition names are displayed (along with partition numbers) in various reports and menus provided by the service processor, Boot Console Handler (BCH), and the HP-UX nPartition tools. Note that some utilities display only the first 30 characters of nPartition names.

Renaming an nPartition [BCH]

Use the Configuration menu `PD` command to check and sets the local nPartition's name from the BCH interface.

Step 1. Login to the service processor for the server complex in which the nPartition resides.

Step 2. Access the nPartition's console.

From the service processor Main menu, enter `CO` to access the console menu and select the nPartition.

If necessary, type `^ecf` (**Control-e c f**) to get write access for the console.

Note that if the nPartition is booted to HP-UX, you should instead use the HP-UX command method of modifying the nPartition name.

Step 3. Access the BCH interface's Configuration menu.

From the Main menu, enter **CO** to access the Configuration menu.

If at another BCH menu, enter `MA` to access the Main menu, then enter `CO` for the Configuration menu.

Step 4. At the BCH Configuration menu, use the **`PD`** command to check and set the local nPartition's name.

Enter `PD` to check the current name, or enter `PD` *`New Name`* to set the nPartition's name to the new name. No quotation marks are needed when specifying the new name.

```
Configuration Menu: Enter command > PD

Partition Number: 1
  Partition Name: Partition 1
Configuration Menu: Enter command >

Configuration Menu: Enter command > PD My New Name

  Partition Name: My New Name
Configuration Menu: Enter command > PD

Partition Number: 1
  Partition Name: My New Name
Configuration Menu: Enter command >
```

Renaming an nPartition [HP-UX]

Use the **`parmodify -p# -P`** ***`name`*** command to set the nPartition name for nPartitions using HP-UX commands.

Step 1. List the current nPartition states and names using the `parstatus -P` command.

This shows all nPartitions, their current status (active or inactive), and their partition numbers and nPartition names.

Step 2. Use the `parmodify -p# -P` *name* command to set the nPartition name for any of the nPartitions in the server complex.

Specify both the partition number (`-p#`) and the new name for the nPartition (`-P` *name*). If the nPartition name contains spaces then quotation marks must surround the name.

SS 21

```
# parmodify -p1 -P "New Name"
Command succeeded.
#
```

You can list the nPartition's new name by using the `parstatus -p#` command or `parstatus -P`.

Renaming an nPartition [Partition Manager]

Use the **Partition —> Modify Partition** action, **General** tab to name and rename nPartitions using Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. In the Partition Manager primary window, select the nPartition whose name you want to change.

Click the nPartition's name in the list on the left side of the primary window to select the nPartition.

Step 3. Select the **Partition —> Modify Partition** action, and access the **General** tab.

The nPartition name is listed—and can be edited—in the Partition Name field in the **General** tab.

Step 4. Edit the nPartition's name in the Partition Name field, and click **OK** when done editing the name (or click **Cancel** to cancel any changes).

Step 5. Review any Notes and Warnings that Partition Manager presents, and click **OK** to implement the name change (or click **Cancel** to cancel the change).

If there are any important notes or warnings, Partition Manager presents them in the window before completing the changes.

When the name change is complete, Partition Manager presents a final dialog box confirming that the nPartition was successfully modified.

Me

SS10

Setting and Checking Cell Attributes

Each cell assigned to an nPartition has *use-on-next-boot* and *failure usage* attributes that determine how the cell is used within the nPartition.

You can list and set cell attributes by using these procedures:

- *Setting Cell Attributes [BCH]* on page 287
- *Setting Cell Attributes [HP-UX]* on page 289
- *Setting Cell Attributes [Partition Manager]* on page 292

Each cell's use-on-next-boot and failure usage attribute settings establish the following behaviors for the cell:

- **Use-on-Next-Boot**

  The use-on-next-boot setting for each cell indicates whether the cell will be used (active) the next time the cell's nPartition is booted.

- **Failure Usage**

  The failure usage setting (called the "Failure Mode" in Partition Manager) for each cell indicates whether the cell will be used, if possible, if any processors or memory fail during the cell's self-tests.

NOTE Currently, only one failure usage setting is supported: *reactivate with interleave* (`ri`).

The reactivate-with-interleave setting allows a cell to actively join its nPartition following processor or memory failures during the cell's self tests. The cell joins its nPartition if at least one processor and any valid amount of memory passes self tests. Any of the cell's components that fail (processors or memory) are not available to the nPartition.

After changing a cell's attributes, the new attribute settings are used starting the next time the nPartition and cells are rebooted.

5509
21

Setting Cell Attributes [BCH]

Use the Configuration menu **CELLCONFIG** command to list and set a cell's use-on-next-boot setting from the BCH interface.

From the BCH interface you can modify only cell use-on-next-boot settings.

Step 1. Login to the complex's service processor, access the nPartition's console, and access the BCH interface.

From the nPartition console, you access the nPartition's BCH interface. If the nPartition is not at the BCH interface, you must either boot the nPartition or shut down HP-UX to return to the BCH interface.

Step 2. Access the BCH Configuration menu by entering **CO** from the BCH Main menu.

If you are at a BCH menu other than the Main menu, enter MA to return to the Main menu and then enter CO to access the Configuration menu.

Step 3. From the BCH Configuration menu, use the **CELLCONFIG** command to list or set each cell's use-on-next-boot setting.

To list the use-on-next-boot settings for all cells in the nPartition, issue the CELLCONFIG command with no arguments.

```
Configuration Menu: Enter command > CELLCONFIG

  Cell Configuration Data for Partition
 ----------------------------------------
  Configured Set   : 0x0000000000000050
  Deconfigured Set: 0x0000000000000000
  Free Cell Set    : 0xffffffffffffffaa


       Cab/
 Cell  Slot  Cell State  Configuration Status
 ----  ----  ----------  --------------------
   4   0/4      Alive        Configured
   6   0/6      Alive        Configured

Configuration Menu: Enter command >
```

To change the use-on-next-boot setting for a cell, issue the CELLCONFIG command with arguments: CELLCONFIG *cell* [ON|OFF]

S508

For example, CELLCONFIG 6 OFF sets the use-on-next-boot setting for cell 6 to OFF. This causes the cell to be inactive (not rendezvous and thus not be used) the next time the nPartition boots.

```
Configuration Menu: Enter command > CELLCONFIG 6 OFF

 Are you sure you want to DECONFIGURE cell 6 for next boot?
(y/[n]) >> y
 Cell 6 will be disabled during next reboot.

Configuration Menu: Enter command >
```

Step 4. Reboot the nPartition to use the cells' new use-on-next-boot settings.

If you have changed any cell use-on-next-boot settings for the nPartition, you should reboot the nPartition in either of two ways:

- Use the BCH interface's REBOOT command to perform a reboot.

  If you have only changed cell configurations from ON to OFF, then perform a reboot using the REBOOT command. Any cells set to not be used will still be assigned to the nPartition but will not be used (will not rendezvous) in the nPartition.

- Use the BCH interface's RECONFIGRESET command to put the nPartition in the ready for reconfig state, then use the service processor Command menu's BO command to boot the nPartition.

  If you have changed any cell from OFF ("n", do not use on next boot) to ON ("y", use the cell on next boot), then you must perform these two tasks; this resets and reconfigures the nPartition and boots it.

SS07

BCH

```
Configuration Menu: Enter command > RECONFIGRESET
Reset the partition for reconfiguration of Complex Profile ...
```

Service Processor (GSP or MP)

```
GSP:CM> BO

This command boots the selected partition.

     #    Name
    ---   ----
     0)   jules00
     1)   jules01

    Select a partition number: 1

    Do you want to boot partition number 1? (Y/[N]) y

    -> The selected partition will be booted.
GSP:CM>
```

Setting Cell Attributes [HP-UX]

Use the **parstatus** and **parmodify -p# -m#...** commands to list and set the use-on-next-boot and failure usage settings for cells using HP-UX commands.

Step 1. Login to HP-UX running on the nPartition.

You can login to HP-UX on the nPartition either by connecting with `telnet` or `rlogin`, or by logging in to its complex's service processor and accessing the nPartition's console.

Connecting through the service processor allows you to maintain nPartition console access after HP-UX has shut down.

Step 2. From the HP-UX command line, use the `parstatus` command to list the use-on-next-boot and failure usage attribute settings for cells in the server complex.

You can list and modify any cell's settings from HP-UX running on any nPartition in the server complex.

Use either `parstatus -C` or `parstatus -V -c#` to list the cell attribute settings. The following examples and text describe both these commands.

- A use-on-next-boot value of "yes" means the cell will be active as part of the nPartition the next time the nPartition boots.

SS06

"Yes" is equivalent to a BCH cell configuration value of ON and "no" is equivalent to OFF.

- A failure usage setting of "activate" (equivalent to "ri") indicates that the cell is set to reactivate with interleave in the event of any failure during the cell's self test.

Use the `parstatus -C` command to list the use-on-next-boot setting for all cells, which is shown in the "Use On Next Boot" column.

```
# parstatus -C
[Cell]
                          CPU     Memory                                Use
                          OK/     (GB)                          Core    On
Hardware   Actual         Deconf/ OK/                           Cell    Next Par
Location   Usage          Max     Deconf    Connected To        Capable Boot Num
========== ============ ======= ========= =================== ======= ==== ===
cab0,cell0 active core  4/0/4    2.0/ 0.0 cab0,bay0,chassis1  yes     yes  0
cab0,cell1 absent       -       -         -                   -       -    -
cab0,cell2 active base  4/0/4    2.0/ 0.0 cab0,bay1,chassis3  yes     yes  0
cab0,cell3 absent       -       -         -                   -       -    -
cab0,cell4 active core  4/0/4    2.0/ 0.0 cab0,bay0,chassis3  yes     yes  1
cab0,cell5 absent       -       -         -                   -       -    -
cab0,cell6 active base  4/0/4    2.0/ 0.0 cab0,bay1,chassis1  no      yes  1
cab0,cell7 absent       -       -         -                   -       -    -

#
```

To list a specific cell's failure-usage and use-on-next boot settings, issue the `parstatus -V -c#` command and specify the cell number.

```
# parstatus -V -c2
[Cell]
Hardware Location        : cab0,cell2
Global Cell Number       : 2
Actual Usage             : active base
Normal Usage             : base
Connected To             : cab0,bay1,chassis3
Core Cell Capable        : yes
Firmware Revision        : 6.0
Failure Usage            : activate
Use On Next Boot         : yes
Partition Number         : 0

....

Memory OK     : 2.00 GB
Memory Deconf : 0.00 GB

#
```

5505
21

Step 3. To modify a cell's use-on-next-boot and failure usage attribute settings, use the `parmodify -p# -m#...` command and specify the cell's new settings.

Specify both the `-p` (partition number) and `-m` (modify cell) options when using `parmodify`. The following example modifies cell 2 to not be used the next time its nPartition (partition number 0) boots.

```
# parmodify -p0 -m2:base:n:ri
Command succeeded.
#
```

The `parmodify` command's `-m` option is as follows:

```
    -m cell:[cell_type]:[use_on_next_boot]:[failure_usage]
```

This option specifies the cell ID (*cell*) whose settings are modified using the following arguments.

- The only valid *cell_type* value is base (base cell).
- The valid *use_on_next_boot* values for cells are:

`y`	Participate in reboot (the default).
`n`	Do not participate in reboot.

- The only valid *failure_usage* value for cells is `ri` (reactivate and interleave).

For details, see the *parmodify* (1M) manpage.

Step 4. If you have modified a cell's attribute settings, you must reboot the nPartition to which the cell is assigned for the settings to be used.

Rebooting the cell's nPartition allows the nPartition to use each cell's new attribute settings.

- If a cell's use-on-next-boot setting is changed from "n" (do not use) to "y" (use), you must perform a reboot for reconfig of the cell's nPartition by using the `shutdown -R` command.
- Otherwise, if the cell use-on-next-boot settings are only changed from "y" to "n" then you can perform a standard reboot using the `shutdown -r` command.

SS04

Setting Cell Attributes [Partition Manager]

Use the **Partition —> Modify Partition** action, **Change Cell Attributes** tab to list and set the configurable cell attributes using Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

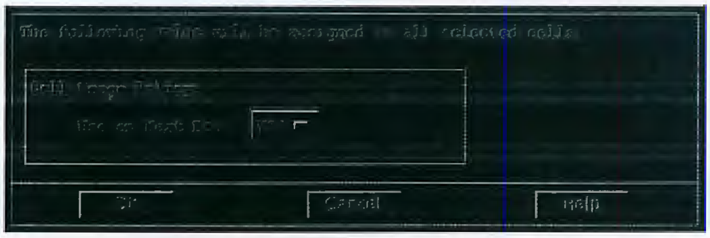
Step 2. In the Partition Manager primary window, select the nPartition whose cell attributes you want to change.

Click the nPartition's name in the list on the left side of the primary window to select the nPartition.

Step 3. Select the **Partition —> Modify Partition** action, and click the **Change Cell Attributes** tab.

Step 4. Highlight the cell whose attributes you want to modify, click the **Modify Cell** button, and configure the cell attributes as desired.

You can modify the settings for multiple cells at once by selecting all desired cells (press **Control** while clicking on the cells) before clicking the **Modify Cell** button.



The following values will be assigned to all selected cells:

Cell Usage Policy

Use on Next Boot: Yes

Configure the cell attributes in the window, and then click **OK** to apply the modified attributes or **Cancel** to cancel any changes.

Step 5. If you have modified any cell attributes, when you return to the **Change Cell Attributes** tab you can click **OK** to apply the changes or click **Cancel** to cancel them.

Review any Notes and Warnings that Partition Manager presents, then click **OK** to proceed or **Cancel** to cancel the changes.

If the cell attribute changes are implemented, Partition Manager presents a final confirmation that the nPartition was successfully modified.

Step 6. If you have modified a cell's attribute settings, you must reboot the nPartition to which the cell is assigned for the settings to be used.

Rebooting the cell's nPartition allows the nPartition to use each cell's new attribute settings.

- If a cell's use-on-next-boot setting is changed from "no" (do not use) to "yes" (use), you must perform a reboot for reconfig of the cell's nPartition by using the `shutdown -R` command.
- Otherwise, if the cell use-on-next-boot settings are only changed from "yes" to "no" then you can perform a standard reboot using the `shutdown -r` command.

5502

Setting and Checking nPartition Core Cell Choices

The **core cell choice** settings for an nPartition are optional preferences that establish which cells in the nPartition are preferred to be selected as the core cell for the nPartition.

You can list and set an nPartition's core cell choices by using these procedures:

- *Setting nPartition Core Cell Choices [BCH]* on page 295
- *Setting nPartition Core Cell Choices [HP-UX]* on page 296
- *Setting nPartition Core Cell Choices [Partition Manager]* on page 297

NOTE

You do not need to specify core cell choices for a valid core cell to be chosen.

By default on HP Superdome and HP rp8400 server, system firmware selects the lowest numbered eligible cell as an nPartition's active core cell. By default on HP rp7405/rp7410 servers, cell 1 is selected as the core cell.

NOTE

You should specify only *core-capable* cells as core cell choices. A cell must have an I/O chassis with core I/O attached to be eligible to be chosen as the core cell.

S501

Setting nPartition Core Cell Choices [BCH]

Use the Configuration menu `COC` command to set the core cell choices for an nPartition using the nPartition's BCH interface.

Step 1. Access the BCH menu for the nPartition whose core cell choices you wish to set.

Step 2. Access the BCH Configuration menu for the nPartition.

From the BCH Main menu, enter `CO` to enter the Configuration menu.

Step 3. Issue the `COC` command to check current core cell choice preferences.

Entering COC with no arguments lists all core cell choice preferences.

Step 4. Issue the `COC` command *with arguments* to set or change the nPartition's core cell choice preferences.

The COC command syntax is: COC *`choice cell`*, where *`choice`* is 0–3 (with 0 being the highest-priority choice) and where *`cell`* is the cell ID.

For example, `COC 0 2` sets the most preferred core cell choice to be cell ID 2. Likewise, `COC 1 4` sets the next (second-highest priority) core preference to be cell ID 4.

Use the HELP COC command for other details about the COC command.

Step 5. [*Optional*] If you have changed the setting for the highest-priority core cell choice (choice 0) and you want the cell you have specified to become the active core cell, then issue the BCH menu's REBOOT command.

Even if you do not perform this step, the new core cell choice settings will be used the next time the nPartition is rebooted.

5500

Setting nPartition Core Cell Choices [HP-UX]

Use the **parstatus** and **parmodify** commands to list and set the core cell choices for an nPartition using HP-UX commands.

Step 1. Issue the **parstatus -V -p#** command to list the nPartition's current core cell choices and core cell use.

The parstatus -V -p# command list detailed status, including the current active core cell ("Core Cell"), and any core cell choice settings (the "Core Cell Alternate" listings, if any).

```
# parstatus -V -p0
[Partition]
Partition Number         : 0
Partition Name           : jules00
Status                   : active
IP address               : 0.0.0.0
Primary Boot Path        : 0/0/2/0/0.13.0
Alternate Boot Path      : 0/0/2/0/0.0.0
HA Alternate Boot Path   : 0/0/2/0/0.14.0
PDC Revision             : 6.0
IODCH Version            : 23664
CPU Speed                : 552 MHz
Core Cell                : cab0,cell0
Core Cell Alternate [1]: cab0,cell0
Core Cell Alternate [2]: cab0,cell2

....

                                      Core Connected  Par
Hardware Location   Usage             IO   To         Num
=================== ============ ==== ========== ===
cab0,bay0,chassis1  active            yes  cab0,cell0 0
cab0,bay1,chassis3  active            yes  cab0,cell2 0

#
```

The core cell choice preferences are listed by parstatus as the "Core Cell Alternate" settings with "1" being the highest priority and "2" through "4" as the lower priority core cell choices.

The parstatus core cell choice listings (1 through 4) directly correspond to the BCH core cell choice listings (0 through 3).

Step 2. Modify the nPartition's core cell choices using the **parmodify -p# -r#...** command.

5199

You can modify the core cell choices for the local nPartition or any remote nPartition in the server complex.

Use the following command: `parmodify -p# -r# -r#...`

Specify the partition number (`-p#`) and the cell ID (`-r#`) for all cells you wish to designate as core cell choices.

```
# parmodify -p0 -r2 -r0
Command succeeded.
#
```

The order in which you list the cells is the order in which the nPartition's core cell choices are established; the first cell listed is the first preferred core cell (choice 1), and the subsequent cells are lower-priority core cell choices (choices 2 through 4, if specified).

Step 3. [*Optional*] If you wish to immediately use the new core cell choice settings, reboot the nPartition whose core cell choices you have changed.

Even if you do not reboot now, the new core cell choices will be used the next time the nPartition is rebooted.

You can issue the `shutdown` command with the `-r` option to reboot the nPartition and use the new core cell choice settings. (You *do not* need to perform a reboot for reconfig of the nPartition.)

If you have modified an *inactive remote* nPartition, use the service processor Command menu's `BO` command to boot the remote nPartition; the designated core cell choices will be used to select the active core cell.

Setting nPartition Core Cell Choices [Partition Manager]

Use the **Partition —> Modify Partition** action, **Cell Cell Choices** tab to set the core cell choices for an nPartition using Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. In the Partition Manager primary window, select the nPartition whose core cell choices you want to change.

Click the nPartition's name in the list on the left side of the primary window to select the nPartition.

Step 3. Select the **Partition —> Modify Partition** action, and click the **Cell Cell Choices** tab.

Step 4. Modify the core choice setting for each cell whose core choice priority you want to revise.

Highlight the cell whose core cell choice you want to configure, select the desired choice priority (1st, 2nd, none, etc.) from the Core Cell Choice pop-up list, and click the **Modify** button to modify the priority.

Step 5. Click the **OK** button when done changing the core choice priorities (or click **Cancel** to not revise any priorities).

Review any Notes and Warnings that Partition Manager presents, then click **OK** to proceed or **Cancel** to cancel the changes.

If the cell choice priority changes are implemented, Partition Manager presents a final confirmation that the nPartition was successfully modified.

The new core cell choice priorities will be used the next time the nPartition is rebooted.

5497

Reassigning (Moving) a Cell to a Different nPartition

To move a cell from one nPartition to another nPartition in the same server complex, use the high-level procedure described here.

This high-level procedure involves:

1. Removing (unassigning) the cell from its original nPartition.
2. Performing a reboot for reconfig (`shutdown -R`) of the original nPartition, if needed.
3. Adding (assigning) the cell to the new nPartition.
4. Performing a reboot for reconfig (`shutdown -R`) of the cell's new nPartition.

Be aware that this procedure modifies the hardware configurations of both nPartitions involved.

You should *adhere to the hardware requirements and performance guidelines* when removing the cell from its original nPartition *and* when adding it to its new nPartition.

When you remove a cell from an nPartition, any I/O connected to the cell also is removed from the nPartition. As a result, any I/O devices associated with the cell are made unavailable to the nPartition.

CAUTION

Moving a cell that has an attached I/O chassis from one nPartition to another is effectively the same as moving the associated I/O devices from one computer to another.

All precautions you would take when moving I/O devices from one computer to another must be taken in this situation.

For example, LVM volume groups that are being moved from one nPartition to another must be exported from their original nPartition *before the cell or I/O chassis is moved*. For details see the *vgexport* (1M) manpage and *Managing Systems and Workgroups*.

S496

Reassigning (Moving) a Cell to a Different nPartition

The following high-level procedure moves a cell to a different nPartition.

You can perform these steps using either HP-UX commands or Partition Manager.

Step 1. See the procedure *Unassigning (Removing) Cells from an nPartition* on page 270 to remove the cell that you want to move to the other nPartition.

As part of this step, you perform a reboot for reconfig (`shutdown -R`) of the nPartition to which the cell is originally assigned.

As a result of this step, the cell is unassigned (on the "free cell list" of available resources) so is is available to be assigned to the other nPartition in the next step.

Step 2. See the procedure *Assigning (Adding) Cells to an nPartition* on page 266 to assign the cell you made available in *Step 1* to its new nPartition.

This step also requires that you perform a reboot for reconfig (`shutdown -R`) of the nPartition to which the cell is being added.

Following the reboot for reconfig, the cell is available (assigned and active) in the new location.

5495

Restoring a Complex Profile

You can restore a previous Complex Profile configuration, which effectively allows you to undo your last nPartition configuration change.

Restoring the previous Complex Profile allows you to revert to the previous complex configuration—including the nPartition configurations—that existed before you made your last change.

NOTE Because restoring a prior Complex Profile requires shutting down all nPartitions to an inactive ready for reconfig state, you should use this procedure only when absolutely necessary.

Restoring a Complex Profile [Service Processor]

Use the Command menu `CC` command and `L` option to restore the prior complex configuration that existed before you made your last nPartition configuration change.

Step 1. Ensure that all nPartitions within the server complex are inactive at the ready for reconfig state.

You can put each nPartition into the ready for reconfig state by using the `shutdown -R -H` command, the BCH interface's `RECONFIGRESET` command, or using the service processor Command menu's `RR` command.

Step 2. Login to the server complex's service processor, and enter `CM` to access the Command menu.

Login as a user with administrator privileges, which are required for restoring the previous complex profile configuration.

Step 3. Issue the `CC` command, select Last Complex Profile (`L`), and confirm that you want to modify the Complex Profile configuration.

```
GSP:CM> CC

This command allows you to change the complex profile.

WARNING: You must either shut down the OSs for reconfiguration or
         execute the RR (reset for reconfiguration) command for all
         partitions before executing this command.
```

```
    G - Build genesis complex profile
    L - Restore last complex profile
        Select profile to build or restore: L

    Do you want to modify the complex profile? (Y/[N]) y

    -> The complex profile will be modified.
GSP:CM>
```

Step 4. Confirm that the nPartition cell assignments are what you intended to establish.

Use the service processor Command menu's **CP** command to display the current complex profile configuration.

```
GSP:CM> CP

--------------------------------------------------------------------------------
Cabinet |    0    |    1    |    2    |    3    |    4    |    5    |    6    |    7
--------+---------+---------+---------+---------+---------+---------+---------+--------
 Slot   |01234567|01234567|01234567|01234567|01234567|01234567|01234567|01234567
--------+---------+---------+---------+---------+---------+---------+---------+--------
 PD  0  |X.X.....|........|........|........|........|........|........|........
 PD  1  |....X.X.|........|........|........|........|........|........|........
 PD  2  |.X.X....|........|........|........|........|........|........|........
 PD  3  |.....X.X|........|........|........|........|........|........|........

GSP:CM>
```

If the nPartition cell assignments are not what you intended—that is, if you prefer the nPartition configuration you had before you restored the existing nPartition configuration—you can repeat this procedure to restore the configuration you had before beginning the procedure.

One level of undo is provided by the service processor Command menu's CC command. This allows you to undo your last nPartition change, and undo your undo.

Step 5. Issue the BO command to boot any nPartitions you want to make active.

After you use the CC command, all nPartitions still are in a boot-is-blocked ready for reconfig state and thus are *inactive* nPartitions.

You can use the Command menu's BO command to boot the nPartitions past boot-is-blocked to make the nPartitions active.

Unlocking Complex Profiles

This section describes how you can force-unlock portions of the nPartition Complex Profile data

CAUTION Do not force-unlock complex profile data except in extremely rare cases following nPartition or server crashes.

Improperly force-unlocking complex profiles can result in the loss of pending configuration changes to nPartitions and the server complex.

Under normal circumstances you do not need to manually unlock the Complex Profile. The commands, utilities, and related procedures handle all locking and unlocking.

In some situations, you must perform a reboot for reconfig (`shutdown -R`) of a modified nPartition in order to complete an nPartition reconfiguration and unlock the changed portion of the Complex Profile. (For example, when removing an active cell from an nPartition you must perform a reboot for reconfig.)

HP-UX provides the `parunlock` command to force-unlock parts of a server's Complex Profile in situations where the normal procedures and utilities have failed.

The service processor (GSP or MP) also provides the `RL` command for resetting Complex Profile locks.

SU92
21

7 Listing and Managing Server Hardware

This chapter covers the tools and procedures for listing details about the hardware assigned to nPartitions. This chapter also covers getting information about server hardware, and managing the hardware resources in nPartitions and their server complexes.

For an introduction to nPartition servers and hardware features, refer to the chapter *nPartition System Overviews* on page 31.

Tools for Listing and Managing Hardware

You can use several software tools to list server hardware details and manage the hardware in a server complex. These tools have features that overlap for some tasks, but each tool also has unique features.

The tools for listing and managing system hardware are:

- **Service Processor (GSP or MP) menus**

  Service processor menus provide a complex-wide service interface that can allow access to all hardware and nPartitions.

NOTE

The service processor in HP servers is sometimes called the Management Processor (MP) and sometimes the Guardian Service Processor (GSP).

Regardless of the name, the service processor in these servers provides approximately the same features and performs essentially the same role.

Throughout this document, the term “service processor” refers to both the MP and GSP service processors.

  Hardware management features include the service processor Command menu’s `DU`, `ID`, `PE`, `PS`, and `SYSREV` commands.

- **Boot Console Handler (BCH) interfaces**

  The BCH interface is the method for interacting with an nPartition before it has booted HP-UX.

  Hardware management features include the BCH interface’s Configuration menu, Interface menu, and Service menu.

- **HP-UX Commands**

  HP-UX commands allow you to manage and monitor nPartitions and hardware within a server complex from HP-UX running on any of the server’s nPartitions.

  Hardware management features include the `parstatus`, `frupower`, `fruled`, and `rad` commands, among many others.

- **Partition Manager** (`/opt/parmgr/bin/parmgr`)

  Partition Manager provides a graphical interface for managing and monitoring nPartitions and hardware within a server complex.

  Hardware management features include menus and windows that list details about cells, I/O chassis, and PCI I/O card slots in the server complex.

- **System Administration Manager** (SAM, `/usr/sbin/sam`)

  The SAM graphical interface (GUI) provides an alternate way to launch Partition Manager as a SAM area.

  SAM also provides a Peripheral Devices area, which has a Cards subarea that is the recommended method for managing PCI I/O cards and PCI slots.

  The **Peripheral Devices —> Cards** area includes error checking and resource analysis not available from the HP-UX command line.

Powering Server Cabinets On and Off

You can power on and power off the cabinets within a server complex either by using the main power switch on the front of the cabinet, or by using the service processor Command menu.

You can use the following procedures:

- *Powering Server Cabinets On and Off [Power Switch]* on page 309
- *Powering Server Cabinets On and Off [Service Processor]* on page 310

When powering off a cabinet, you turn off 48-volt power to the cabinet thus causing all cells and all I/O chassis to power off, and causing most fans to turn off.

CAUTION

When you power on or off HP Superdome 64-way compute cabinets, you must power off and power on cabinet 0 and cabinet 1 in such a way that *both cabinets are off* for an overlapping interval.

If either Superdome 64-way cabinet is powered off then powered on while the other cabinet remains on, then communications between the two cabinets is lost.

CAUTION

Before powering off system hardware, you first must check whether it is being used.

The cabinet power switch and the service processor Command menu's `PE` command *do not check* whether system hardware is in use before powering it off.

Changes in cabinet power status *do not* affect the standby power that supplies system utilities such as the service processor (GSP or MP) and keeps some fans running. These utilities and fans can receive power as long as standby power is enabled.

The way in which standby power is enabled and disabled differs for various HP server models. On HP Superdome servers, standby cabinet power is switched using the power breakers on the rear of the cabinet. On HP rp7405/rp7410 and HP rp8400 servers, standby power is enabled through the power cords connecting to the inputs on the rear of the cabinet.

Powering Server Cabinets On and Off [Power Switch]

Use the Virtual Front Panel to check status, and then use the cabinet power switch to manage a cabinet's 48-volt power with the cabinet hardware.

Step 1. Login to the system's service processor and access the Virtual Front Panel for the system.

From the service processor Main menu, enter `VFP` to access the Virtual Front Panel menu, then enter `S` to access the "system VFP" that displays the current status for all nPartitions.

Step 2. Check the VFP status to see whether any cabinet hardware is running HP-UX.

Any nPartition whose state is "HP-UX heartbeat" is running HP-UX and thus should not have its hardware powered off until after HP-UX is shut down.

Type `^b` (**Control-b**) to exit the VFP.

Step 3. Shut down HP-UX running on any cabinet hardware that you plan to power off.

Step 4. Confirm that nobody else is using or servicing the cabinet hardware you plan to power on or off.

You should both physically inspect the hardware, and check whether others are remotely accessing the system's service processor (using the Command menu's `WHO` command).

Step 5. Access the cabinet hardware and flip the power switch (located on the cabinet's front) to the on or off position in order to power the cabinet on or off.

S486

Powering Server Cabinets On and Off [Service Processor]

Use the Virtual Front Panel, and the use the Command menu **PE** command to turn a cabinet's 48-volt power on or off from the service processor (GSP or MP).

Step 1. Login to the system's service processor and access the Virtual Front Panel for the system.

From the service processor Main menu, enter **VFP** to access the Virtual Front Panel menu, then enter **S** to access the "system VFP" that displays the current status for all nPartitions.

Step 2. Check the VFP status to see whether any cabinet hardware is running HP-UX.

Any nPartition whose state is "HP-UX heartbeat" is running HP-UX and thus should not have its hardware powered off until after HP-UX is shut down.

Step 3. Shut down HP-UX running on any cabinet hardware that you plan to power off.

Step 4. Confirm that nobody else is using or servicing the cabinet hardware you plan to power on or off.

You should both physically inspect the hardware, and check whether others are remotely accessing the system's service processor (using the Command menu's **WHO** command).

Step 5. Access the system's service processor Command menu, issue the **PE** command, then select the cabinet to power on or power off.

From the service processor Main menu, enter **CM** to access the Command menu. To exit the Command menu enter **MA**.

When using the `PE` command enter **B** to power on or off a cabinet; specify the cabinet number; and then enter **ON** (power on), **OFF** (power off), or **Q** (quit without changing the power status).

```
GSP:CM> PE

This command controls power enable to a hardware device.

    B - Cabinet
    C - Cell
    I - IO Chassis
        Select Device: b
```

```
Enter cabinet number: 1

The power state is ON for Cabinet 1.
In what state do you want the power? (ON/OFF)
```

Powering Cells and I/O Chassis On and Off

This section covers *cell* and *I/O chassis* power management procedures, which allow you to control power for cells and I/O chassis from remote locations, without physically accessing the system hardware.

You can use the following procedures:

- *Powering Cells and I/O Chassis On and Off [Service Processor]* on page 313
- *Powering Cells and I/O Chassis On and Off [HP-UX]* on page 314
- *Powering Cells and I/O Chassis On and Off [Partition Manager]* on page 316

NOTE

On HP nPartition systems, *powering on* a cell also powers on any I/O chassis attached to the cell, and *powering off* a cell also powers off any I/O chassis attached to the cell.

Powering on or off an I/O chassis connected to a powered-on cell *causes the cell to reset* if the cell located and mapped the I/O chassis during its cell boot process.

The `frupower` command and Partition Manager permit you to power on or off *inactive* cells and I/O chassis that are assigned to the current nPartition or are not assigned to any nPartition.

The service processor Command menu's `PE` command permits you to power on or off any hardware in the complex, including active cells and I/O chassis. The `PE` command does not check the current usage of components.

5483

21

Powering Cells and I/O Chassis On and Off [Service Processor]

Use the Command menu **PE** command to power on and power off cells, I/O chassis, and cabinets from the service processor interface (GSP or MP).

CAUTION When using the service processor Command menu's PE command to power on or off hardware, you should be certain to *specify the correct component* to power on or off.

The PE command *does not check* whether the hardware is actively being used.

You can manage the power for all components within the system complex using the service processor Command menu's PE command, regardless of any nPartition assignment or the status (active or inactive) for the hardware components.

Step 1. Login to the system's service processor and access the Command menu.

From the service processor Main menu, enter **CM** to access the Command menu. To exit the Command menu enter **MA**.

Step 2. Issue the **PE** command and specify the type of hardware whose power you want to turn on or turn off.

You can manage power to cells, I/O chassis, and cabinets.

Step 3. Specify the hardware device to power on or power off.

The service processor *does not check* whether the specified component is currently being used.

- **Cabinets**—When you power on or off a cabinet, the firmware also powers on or off all cells and I/O chassis in the cabinet.
- **Cells**—When you power on or off a cell, the firmware also powers on or off any I/O chassis attached to the cell.

  When specifying a cell, you indicate both the *cabinet number* and the *slot* in which the cell resides.

5982

- **I/O Chassis**—When you power off an I/O chassis from the service processor Command menu, the system firmware *resets the cell* attached to the I/O chassis (if the cell located and mapped the I/O chassis during its cell boot process).

  When specifying an I/O chassis, you indicate the cabinet, bay, and chassis numbers to identify it.

In the following example, the service processor powers off cell 2 in cabinet 0.

```
GSP:CM> PE

This command controls power enable to a hardware device.

    B - Cabinet
    C - Cell
    I - IO Chassis
        Select Device: c

    Enter cabinet number: 0
    Enter slot number: 2

    The power is ON for the Cell in Cabinet 0, Slot 2.
    In what state do you want the power for the
    Cell in Cabinet 0, Slot 2? (ON/OFF) OFF


GSP:CM>
```

Powering Cells and I/O Chassis On and Off [HP-UX]

Use the **`frupower -o -c#`** and **`frupower -f -c#`** commands to power on and power off cells (and their associated I/O chassis) from HP-UX.

NOTE

You can use the `frupower` command to power on or off *inactive cells* that are either assigned to the local nPartition or are not assigned to an nPartition.

You cannot power off active cells or power on or off cells assigned to a remote nPartition when using `frupower`.

To power on or off an I/O chassis using `frupower`, do so by power cycling the cell to which it is connected.

Step 1. Login to HP-UX running on one of the system's nPartitions.

To manage a cell's power, you must login to the nPartition to which the cell is assigned. If the cell is not assigned to an nPartition, you can manage its power from *any* nPartition.

Step 2. Use the `frupower` command to turn on or turn off the cell's power.

Specify the **`frupower -f -c#`** command to *power off* a cell. (`-c#`). This also powers off any I/O chassis connected to the cell.

Specify the **`frupower -o -c#`** command to *power on* a cell (`-c#`). This also powers on any I/O chassis connected to the cell.

The following example shows several sample `frupower` commands and their results.

```
# frupower -f -c0
Error: Can not power off active cell 0.
# frupower -f -c2
# frupower -o -c2
# frupower -f -c6
Error: Cell 6 belongs to partition 1.  Can not power off cell.
#
# frupower -f -i0/1/1
Error: I/O chassis 0/1/1 is attached to a powered-on free
cell 4.  Please power off the free cell.
#
```

In the above example, cell 0 is active and thus cannot be powered off using `frupower`. Cell 2 is inactive and is powered off (`frupower -f -c2`) and then powered back on (`frupower -o -c2`). Cell 6 is assigned to a remote nPartition (partition number 1) and thus cannot be powered off. I/O chassis 0/1/1 is attached to cell 4, so to power it off cell 4 must be powered off.

Powering Cells and I/O Chassis On and Off [Partition Manager]

Use the **Cell —> Power On Cell** action, or **Cell —> Power Off Cell** action, to power on and power off cells (and their associated I/O chassis) from Partition Manager.

NOTE You can use Partition Manager to power on or off *inactive cells* that are assigned to the local nPartition.

You cannot power off active cells or power on or off cells assigned to a remote nPartition when using Partition Manager.

To power on or off an I/O chassis using Partition Manager, do so by power cycling the cell to which it is connected.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. Select the nPartition that contains the cell you want to power on or off.

Partitions are listed on the left side of the Partition Manager primary window.

The cells and I/O chassis assigned to the nPartition are listed on the right side of the primary window once the nPartition is selected.

Step 3. Select the cell whose power you want to turn on or off.

Step 4. Select the **Cell —> Power On Cell** menu item, or select the **Cell —> Power Off Cell** menu item.

Power Status for Hardware Components

You can use system software to check power status for the following components from remote locations:

- Cabinets
- Bulk Power Supplies and Power Boards
- Cell Boards
- I/O Chassis
- Individual PCI Slots

NOTE Cabinet power details and power supply details are specific to each server model. For example, HP Superdome servers and HP rp8400 server have different power configurations and requirements.

You can use the following procedures:

- *Determining Hardware Power Status [Service Processor]* on page 318
- *Determining Hardware Power Status [HP-UX]* on page 320
- *Determining Hardware Power Status [Partition Manager]* on page 322

S478

Determining Hardware Power Status [Service Processor]

Use the Command menu **PS** command to check power status for cabinets, bulk power supplies and power boards, cells, and core I/O from the service processor.

Step 1. Login to the system's service processor and enter **CM** to access the Command menu.

Step 2. Issue the service processor Command menu's **PS** command.

The PS command can list detailed information—including power status—for components within the system complex.

The PS command summarizes all cabinets, cells, and core I/O cards, and prompts you to specify which hardware device you want information about.

```
GSP:CM> PS

This command displays detailed power and hardware configuration status.

The following GSP bus devices were found:
+----+-----+-----------+---------------+-----------------------------------+
|    |     |           |               |              Core IOs             |
|    |     |           |               | IO Bay  | IO Bay  | IO Bay  | IO Bay |
|    |     |   UGUY    |     Cells     |    0    |    1    |    2    |    3   |
|Cab.|     |           |               |IO Chas. |IO Chas. |IO Chas. |IO Chas.|
| #  | GSP | CLU | PM  |0 1 2 3 4 5 6 7|0 1 2 3  |0 1 2 3  |0 1 2 3  |0 1 2 3 |
+----+-----+-----+-----+---------------+---------+---------+---------+--------+
|  0 |  *  |  *  |  *  |* * * * * * * *|  *   *  |         |         |        |
|  1 |     |  *  |  *  |* * * * * * * *|  *   *  |         |         |        |
|  8 |     |  *  |  *  |               |  *   *  |  *   *  |         |        |
You may display detailed power and hardware status for the following items:

    B - Cabinet (UGUY)
    C - Cell
    G - GSP
    I - Core IO
        Select Device:
```

Step 3. Specify the cabinet whose hardware and power status you want to check.

For each cabinet (B), the PS command reports detailed information that includes the power status for *all components* within the cabinet, including:

- **Cabinet Power**—Whether the 48-volt cabinet power switch is on or off, whether cabinet power is enabled, and details about power boards and bulk power supplies.
- **Cell Power**—Whether power is enabled and on for all cells within the cabinet.
- **Core I/O Card Power**—Whether power is enabled and on for all core I/O cards within the cabinet.

For system complexes that have multiple cabinets, you must check details for each cabinet separately.

You also can use the `PS` command to check individual cell (`C`) or core I/O (`I`) hardware and power status.

The following example shows cabinet power details for cabinet 0 of an SD64000 model Superdome server.

```
 Select Device: b

    Enter cabinet number: 0

HW status for SD64000 compute cabinet #0: NO FAILURE DETECTED
Power switch: on;  Power: enabled, good;  Door: closed
Fan speed: normal;  Temperature state: normal
Redundancy state: fans or blowers redundant, BPSs redundant

                      | Main BP|                 |    IO Backplanes      |
                      | Power  |                 | IO Bay 0 | IO Bay 1   |
               | Main | Boards |      Cells      | Chassis  | Chassis    |
               | BP   | 0 1 2  | 0 1 2 3 4 5 6 7 | 0 1 2 3  | 0 1 2 3    |
+--------------+------+--------+-----------------+----------+------------+
 Populated     |  *   | * * *  | * * * * * * * * |   *   *  |            |
 Power Enabled |  *   | * * *  | * * * * * * * * |   *   *  |            |
 Powered On    |  *   | * * *  | * * * * * * * * |   *   *  |            |
 Power Fault   |      |        |                 |          |            |
 Attention LED |      |        | *               |   *      |            |

                          | Cabinet | IO        |
            |     BPS     | Blowers |  Fans     |
            | 0 1 2 3 4 5 | 0 1 2 3 | 0 1 2 3 4 |
+-----------+-------------+---------+-----------+
  Populated | * * * * *   | * * * * | * * * * * |
  Failed    |             |         |           |
```

5476

Determining Hardware Power Status [HP-UX]

Use the `parstatus -B`, `parstatus -V -b#`, `frupower -d -C`, `frupower -d -I`, or `rad -q` command to check the power status for system hardware from HP-UX.

For details on these HP-UX commands, see the online manpages for *parstatus* (1M), *frupower* (1M), and *rad* (1M).

Step 1. Login to HP-UX running on one of the system's nPartitions.

To check the power status for PCI card slots, you must login to the *local nPartition* where their PCI card cage resides.

You can check the power status for cabinets, cells, and I/O chassis from *any nPartition*.

Step 2. Issue the HP-UX commands to check the power status for the system components of interest to you.

- **Cabinet Power**—Use the `parstatus -V -b#` command to check cabinet power status for the specified cabinet (`-b#`), or use the `parstatus -B` command for brief power status for all cabinets.

  The `parstatus` command gives details about each cabinet's bulk power supplies and power boards, as well as details about cabinet fans and blowers.

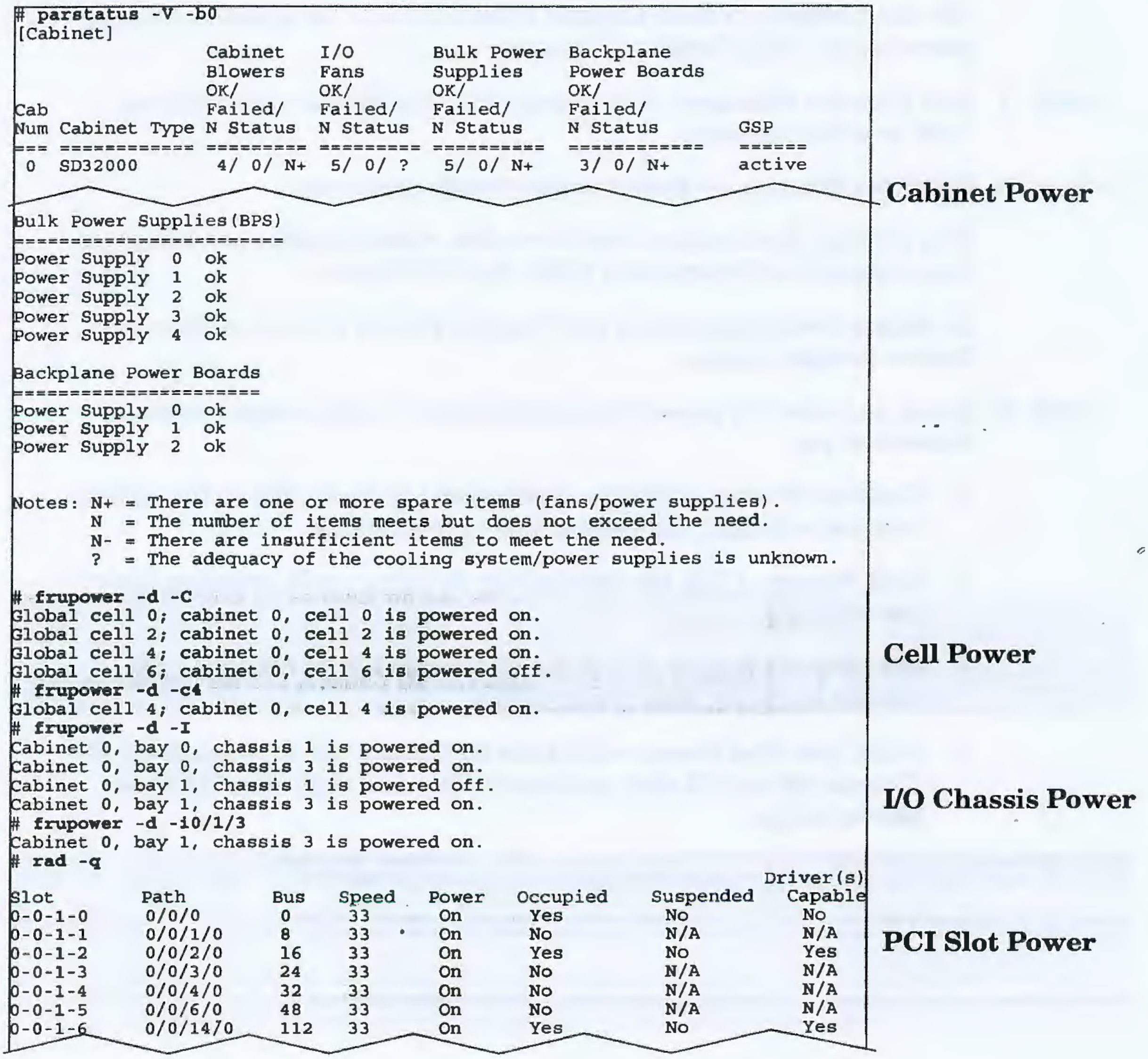
- **Cell Power**—Use the `frupower -d -C` command to list cell power status for all cells, or use the `frupower -d -c#` command to list power status for a specific cell (`-c#`).

- **I/O Chassis Power**—Use the `frupower -d -I` command for power status for all I/O chassis, or use the use `frupower -d -i#/#/#` command to list details for a specific I/O chassis (*`cabinet/bay/chassis`*)

- **PCI Card Slot Power**—Use the `rad -q` command and option to list details including PCI card slot power for all PCI card slots within the local nPartition.

  The `rad` command lists information for the local nPartition only.

The following example output shows power details for an HP Superdome system's cabinet, cells, I/O chassis, and PCI slots, as presented by various HP-UX commands.



```
# parstatus -V -b0
[Cabinet]
                  Cabinet   I/O       Bulk Power  Backplane
                  Blowers   Fans      Supplies    Power Boards
                  OK/       OK/       OK/         OK/
Cab               Failed/   Failed/   Failed/     Failed/
Num Cabinet Type  N Status  N Status  N Status    N Status     GSP
=== ============  ========= ========= ==========  ============ ======
 0  SD32000        4/ 0/ N+  5/ 0/ ?   5/ 0/ N+    3/ 0/ N+    active

Bulk Power Supplies(BPS)
========================
Power Supply  0  ok
Power Supply  1  ok
Power Supply  2  ok
Power Supply  3  ok
Power Supply  4  ok

Backplane Power Boards
======================
Power Supply  0  ok
Power Supply  1  ok
Power Supply  2  ok


Notes: N+ = There are one or more spare items (fans/power supplies).
       N  = The number of items meets but does not exceed the need.
       N- = There are insufficient items to meet the need.
       ?  = The adequacy of the cooling system/power supplies is unknown.

# frupower -d -C
Global cell 0; cabinet 0, cell 0 is powered on.
Global cell 2; cabinet 0, cell 2 is powered on.
Global cell 4; cabinet 0, cell 4 is powered on.
Global cell 6; cabinet 0, cell 6 is powered off.
# frupower -d -c4
Global cell 4; cabinet 0, cell 4 is powered on.
# frupower -d -I
Cabinet 0, bay 0, chassis 1 is powered on.
Cabinet 0, bay 0, chassis 3 is powered on.
Cabinet 0, bay 1, chassis 1 is powered off.
Cabinet 0, bay 1, chassis 3 is powered on.
# frupower -d -i0/1/3
Cabinet 0, bay 1, chassis 3 is powered on.
# rad -q
                                                                Driver(s)
Slot        Path        Bus    Speed   Power   Occupied   Suspended   Capable
0-0-1-0     0/0/0       0      33      On       Yes        No          No
0-0-1-1     0/0/1/0     8      33      On       No         N/A         N/A
0-0-1-2     0/0/2/0     16     33      On       Yes        No          Yes
0-0-1-3     0/0/3/0     24     33      On       No         N/A         N/A
0-0-1-4     0/0/4/0     32     33      On       No         N/A         N/A
0-0-1-5     0/0/6/0     48     33      On       No         N/A         N/A
0-0-1-6     0/0/14/0    112    33      On       Yes        No          Yes
```

Determining Hardware Power Status [Partition Manager]

Use the **Complex —> Show Complex Details** menu to list system hardware power status using Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. Select the **Complex —> Show Complex Details** menu item.

This displays the Complex Details window, which has tabs providing info for cabinets (the General tab), Cells, and I/O Chassis.

To update the information in the Complex Details window, click the the **Rescan Complex** button.

Step 3. Select and view the power status information for the components of interest to you.

- **Cabinet Power**—Click the **Cabinet Info** tab for details on the system complex's cabinet, including cabinet power status.
- **Cell Power**—Click the **Cells** tab for details on cells including their power status.
- **I/O Chassis Power**—Click the **I/O Chassis** tab for details on I/O chassis including their power status.
- **PCI Card Slot Power**—Click the **I/O Chassis** tab, then select the I/O Chassis whose PCI slots you want to list, and then click the **Show Details** button.

Turning Attention Indicators (LEDs) On and Off

HP's nPartition systems provide **attention indicators (LEDs)** to help you to visually select and confirm which hardware you want to perform operations on. Attention indicators are amber (orange) lights.

Table 7-1 on page 324 lists attention indicator meanings and LED states (off, blinking, and on). These states and meanings adhere to the PCI Hot-Plug specification.

You can control the attention indicators for various hardware components by using the following procedures:

- *Turning Attention LEDs On and Off [HP-UX]* on page 325
- *Turning Attention LEDs On and Off [Partition Manager]* on page 327

NOTE On HP Superdome servers, the attention indicator behavior has changed since the original HP-UX 11i release.

Starting with the June 2001 HP-UX 11i release, the HP-UX command and utility behavior is to blink attention indicators (rather than light them to a steady-on state, as was the original behavior).

As a result, HP Superdome servers upgrading to the June 2001 or later release will exhibit the new, blinking behavior (see Table 7-1 on page 324) when cell and I/O chassis attention indicators are enabled.

In cases where some nPartitions are running the original HP-UX 11i release and others are running a more recent release, *both behaviors* (the original "steady-on" behavior and the "PCI Hot-Plug" behavior) may be exhibited—possibly within the same server complex.

Table 7-1 lists the meanings for the various attention indicator states. When all of a system's components are functioning and no service operations are occurring, every attention indicator should be turned off. (HP Superdome cabinet number LCDs remain lit or blinking when cabinet power is on.)

Table 7-1 **Attention Indicator (LED) States and Meanings**

Attention Indicator State	Meaning
OFF	Not selected.
BLINKING	Selected to be used in a service operation.
ON	*Supported for PCI card slot LEDs only.* Service required, problems have been identified with the component.

LEDs for Hardware Components

You can control (turn off, blink, and/or turn on) attention indicators for the following hardware components.

- **Cell LEDs**

  Each cell or cell slot has its own attention indicators.

  — On HP *Superdome servers*, each cell's attention indicator is located on the server cabinet hardware below the cell's slot, just to the right of the cell slot's power LED.

  — On HP *rp7405 / rp7410 and rp8400 servers*, each cell's attention indicator is located on the cell hardware, to the outside of the cell's power LEDs.

- **I/O Chassis LEDs**

  On HP *Superdome servers* only, each I/O chassis has a attention indicator, which is located on the cabinet above the I/O chassis.

- **PCI Card Slot LEDs**

  On *all* HP nPartition systems, each PCI card slot has an attention indicator that you can use to select the card slot. You can view a PCI card slot's attention indicator when accessing the card cage.

S471

On HP *rp7405 / rp7410 and rp8400 servers* only, you also can view each PCI slot's attention indicator beneath the corresponding slot, on the cabinet's external chassis at the rear of the server cabinet.

- **Cabinet Number LCDs**

  On HP *Superdome servers* only, each cabinet has a cabinet number LCD that serves as the cabinet's attention indicator.

NOTE

The **cabinet "attention" light** on HP Superdome, HP rp8400, and HP rp7405/rp7410 servers is not user-controllable.

The cabinet "attention" light automatically turns on when one or more alert level 6 (or higher) chassis codes has been recorded in the error logs and has not yet been read. This light automatically turns off when a user enters the service processor (GSP or MP) chassis logs viewer.

Turning Attention LEDs On and Off [HP-UX]

Use the **`fruled -o...`**, **`fruled -f...`**, or **`rad -f...`** command to manage attention indicators by turning them on, off, or blinking them from HP-UX.

Step 1. Login to HP-UX running on one of the system's nPartitions.

You can manage cabinet, cell, and I/O chassis attention indicators from HP-UX on *any nPartition*. To manage PCI slot attention indicators, you must access HP-UX in the *local nPartition* to which the PCI slot's chassis is assigned.

Step 2. Use the `fruled` command or the `rad` command to manage (turn on, off, or blink) the attention indicator for a system hardware component.

From HP-UX you can manage LEDs for the following hardware components:

- **Cells**—Use `fruled` to blink or turn off a cell's attention indicator.

  — Turn Off: The **`fruled -f -c#`** command *turns off* the attention indicator for the specified cell (`-c#`). To turn off all cell attention indicators use the **`fruled -f -C`** command.

S470

  - Blink: The **`fruled -o -c#`** command *blinks* the attention indicator for the specified cell (`-c#`).

- **I/O Chassis**—Use `fruled` to blink or turn off HP Superdome I/O chassis attention indicators.

  Specify the I/O chassis using *`cabinet/bay/chassis`* notation (#/#/#).

  - Turn Off: The **`fruled -f -i#/#/#`** command *turns off* the attention indicator for the specified I/O chassis (`-i#/#/#`). To turn off all I/O chassis attention indicators use the **`fruled -f -I`** command.
  - Blink: The **`fruled -o -i#/#/#`** command *blinks* the attention indicator for the specified I/O chassis (`-i#/#/#`).

- **Cabinet Numbers**—Use `fruled` to blink or not-blink (keep lit) the cabinet number LCD for an HP Superdome cabinet.

  - Not-Blink: The **`fruled -f -b#`** command *stops blinking* (keeps it lit) the cabinet number LCD for the specified cabinet (`-b#`).
  - Blink: The **`fruled -o -b#`** command *blinks* the cabinet number LED for the specified cabinet (`-b#`).

- **PCI Card Slots**—Use `rad` to turn on, off, or blink the attention indicator for a PCI card slot.

  Specify the PCI slot using *`cabinet-bay-chassis-slot`* (#-#-#-#) notation.

  - Turn Off: The **`rad -f off`** ***`slot`*** command *turns off* the attention indicator for the specified PCI card slot (*`slot`*).
  - Blink: The **`rad -f attention`** ***`slot`*** command *blinks* the attention indicator for the specified PCI card slot (*`slot`*).
  - Turn On: The **`rad -f on`** ***`slot`*** command *turns on* the attention indicator for the specified PCI card slot (*`slot`*).

For details see the *fruled* (1) manpage or the *rad* (1M) manpage.

The following example turns off and blinks various attention indicators on an HP Superdome system, including cell, I/O chassis, PCI slot, and cabinet LEDs.

5469
20

`# fruled -f -C`
`# fruled -f -I`
	Turn off all cell and I/O chassis attention

`# fruled -o -c0 -c2 -c4`
`# fruled -o -i0/0/1 -i0/0/3`
`# fruled -o -b0`
	Blink attention indicators for cells 0, 2, and 4 and I/O chassis 0/0/1 and 0/0/3. *Blink* the cabinet number LCD for

`# fruled -f -C`
`# fruled -f -I`
`# fruled -f -b0`
	Turn off all cell and I/O chassis attention indicators and *stop blinking* the cabinet number LED.

`# rad -f attention 0-0-1-2`
`# rad -f off 0-0-1-2`
`#`
	Blink the attention indicator for PCI slot 2 in cabinet 0, bay 0, chassis 1. Then *turn off* the same PCI slot's attention

Turning Attention LEDs On and Off [Partition Manager]

Use the **Cell —> Light Cell LED** action, the **I/O —> Light I/O Chassis LED** action, or the **I/O —> Light Chassis and Slot LEDs** action to manage a hardware component's attention indicator by blinking it and turning it off from Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. In Partition Manager's primary window, select the nPartition to which the hardware component (cell, I/O chassis, or PCI slot) is assigned, or select Available Resources if the component is not assigned.

Step 3. Select the hardware component whose attention indicator you want to blink, then select the appropriate menu item to blink the LED.

You can manage LEDs for the following hardware components:

- **Cells**—Select the cell in Partition Manager's primary window, then select the **Cell —> Light Cell LED** menu item.

5468

This menu item *blinks* the selected cell's attention indicator. On HP Superdome servers this *also blinks* the cabinet number LCD for the cabinet in which the cell resides.

- **I/O Chassis**—Select the I/O chassis in Partition Manager's primary window, then select the **I/O —> Light I/O Chassis LED** menu item.

  On HP Superdome servers this menu item *blinks* the attention indicator for the selected I/O chassis, and *also blinks* the cabinet number LCD for the cabinet in which the I/O chassis resides.

- **PCI Card Slots**—Double-click the PCI slot's I/O chassis in Partition Manager's primary window, then select the PCI slot listed in the I/O chassis window, and then select the **I/O —> Light Chassis and Slot LEDs** menu item.

  This menu item blinks the selected PCI card slot's attention indicator.

  On HP Superdome servers, this also blinks the I/O chassis attention indicator and blinks the cabinet number LCD.

Step 4. Click the **OK** button in the window to *turn off* the attention indicator for the hardware component you selected.

On HP Superdome servers, this *also turns off* any I/O chassis attention indicator and *stops blinking* any cabinet number LCD changed by this procedure.

Listing Cell Processor and Memory Configurations

You can determine the processor and memory configurations for cells in a server complex by using software tools and utilities.

Table 7-2 on page 330 lists the processor version info (HVERSIONs) that is reported by the procedures given in this section.

You can list processor and memory details using the following procedures:

- *Listing Cell Processors and Memory [Service Processor]* on page 331
- *Listing Cell Processors and Memory [BCH]* on page 333
- *Listing Cell Processors and Memory [HP-UX]* on page 334
- *Listing Cell Processors and Memory [Partition Manager]* on page 335

SU66
2

Table 7-2 Processor (CPU) Versions for Cells

Cell's Operating CPU Frequency	HVERSION for HP rp7405/rp7410 and rp8400 Servers	HVERSION for HP Superdome Servers
PA8600 — 552 MHz	—	`0x5c70`
PA8700 — 650 MHz	`0x5e60`	`0x5d70`
PA8700 — 750 MHz	`0x5e40`	`0x5e70`
PA8700 — 875 MHz	`0x5eb0`	`0x5ea0`

PA-RISC Processor HVERSIONs

Table 7-2 lists the processor HVERSION numbers that are reported for nPartitions and cells. These are hexadecimal numbers. HP Superdome processor HVERSIONs differ from rp7405/rp7410 and rp8400 HVERSIONs. See the procedures that follow for info on listing HVERSIONs.

NOTE

The HVERSION indicates the current operating frequency for processors in cells, but does not necessarily indicate the processor hardware revisions.

For a cell that is assigned to an nPartition, the processor HVERSION is based on the *operating frequency of the monarch cell* in the nPartition to which the cell is assigned.

Likewise, for a cell not assigned to an nPartition, the reported HVERSION refers to the *operating frequency of the cell.*

All processors in a cell operate at the same frequency, and all cells in an nPartition must operate at the same frequency. Different nPartitions in a server can operate at different frequencies.

Listing Cell Processors and Memory [Service Processor]

Use the Command menu `PS` command to list cell processor and memory configurations using the service processor Command menu.

Step 1. Login to the system's service processor and enter `CM` to access the Command menu.

You can check processor and memory details for any cell in the complex from the service processor.

Step 2. Issue the `PS` command and specify the cell whose processor and memory details you want to view.

The `PS` command reports details for the cell including its processor configuration (CPU population) and its memory configuration (DIMM population).

For the cell *memory configuration* details, the `PS` command displays each populated DIMM and identifies it using its rank notation (0A–0D, 1A–1D, and so on).

The following example shows details for cell 0 in cabinet 0, which has four processors (0–3) and four DIMMs installed (0A–0D).

5464

```
GSP:CM> PS

This command displays detailed power and hardware configuration status.

You may display detailed power and hardware status for the following items:

    B - Cabinet (UGUY)
    C - Cell
    G - GSP
    I - Core IO
        Select Device: c

    Enter cabinet number: 0
    Enter slot number: 0

HW status for Cell 0 in cabinet 0: NO FAILURE DETECTED

Power status: on, no fault
Boot is not blocked; PDH memory is shared
Cell Attention LED is off
RIO cable status: connected
RIO cable connection physical location: cabinet 0, IO bay 1, IO chassis 3
Core cell is cabinet 0, cell 0

PDH status LEDs:  ****
                             CPUs
                           0 1 2 3
          Populated        * * * *
          Over temperature

DIMMs populated:
+----- A -----+ +----- B -----+ +----- C -----+ +----- D -----+
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
*               *               *               *

PDC firmware rev 10.0
PDH controller firmware rev 7.6, time stamp: TUE MAY 08 20:42:26 2001

GSP:CM>
```

S463

Listing Cell Processors and Memory [BCH]

Use the Information menu **PR** and **ME** commands to list cell processor and memory configurations from an nPartition's BCH interface.

Using the BCH interface, you can check these details only for the active cells in the local nPartition.

Step 1. Access the BCH interface for the nPartition to which the cell is assigned, and access the BCH Information menu.

From the BCH Main menu, enter **IN** to access the BCH Information menu. (If you are not at the BCH Main menu, enter **MA** to go to the Main menu.)

Step 2. From the BCH Information menu, list the processor or memory status for all cells by issuing the **PR** and **ME** commands.

- **Processor status**—Use the **PR** command to report details about all processors on all active cells in the nPartition.
- **Memory status**—Use the **ME** command to report details about all active cells' memory configurations.

  The ME command summarizes memory (DIMM) details for each ranks of memory. Each rank is a set of 4 DIMMs.

These BCH commands do not report details for inactive cells.

```
Information Menu: Enter command > PR

PROCESSOR INFORMATION

        Cab/                                                       Processor
 Cell   Slot    CPU     Speed      HVERSION   SVERSION   CVERSION    State
 ----   ----    ---   ---------    --------   --------   --------  -------------
   4    0/4      0     552 MHz      0x5c70     0x0491     0x0301    Active
                 1     552 MHz      0x5c70     0x0491     0x0301    Idle
                 2     552 MHz      0x5c70     0x0491     0x0301    Idle
                 3     552 MHz      0x5c70     0x0491     0x0301    Idle
   6    0/6      0     552 MHz      0x5c70     0x0491     0x0301    Idle
                 1     552 MHz      0x5c70     0x0491     0x0301    Idle
                 2     552 MHz      0x5c70     0x0491     0x0301    Idle
                 3     552 MHz      0x5c70     0x0491     0x0301    Idle

Information Menu: Enter command > ME

Partition Memory Information
```

5465

```
Cell    DIMM Rank 0/1      DIMM Rank 2/3      DIMM Rank 4/5      DIMM Rank 6/7
       Size   Status      Size   Status      Size   Status      Size   Status
---- ------ ---------  ------ ---------  ------ ---------  ------ ---------
  4  2048MB Active        ---                ---                ---
        ---               ---                ---                ---
  6  2048MB Active        ---                ---                ---
        ---               ---                ---                ---

       Partition Total Memory:     4096
      Partition Active Memory:     4096
Partition Deconfigured Memory:        0

* status is scheduled to change on next boot.

Information Menu: Enter command >
```

Listing Cell Processors and Memory [HP-UX]

Use the **parstatus** command with various options to list cell processor and memory configurations from HP-UX.

You can check these details for any cell in the complex.

Step 1. Login to HP-UX running on any of the system's nPartitions.

You can list processor and memory details from any nPartition.

Step 2. Issue the `parstatus` command to view cell hardware details including processor and memory configurations.

Use any of the following `parstatus` commands to view cell hardware information:

- **parstatus -V -c#**

  List detailed processor and memory configuration information for the specified cell.

- **parstatus -C**

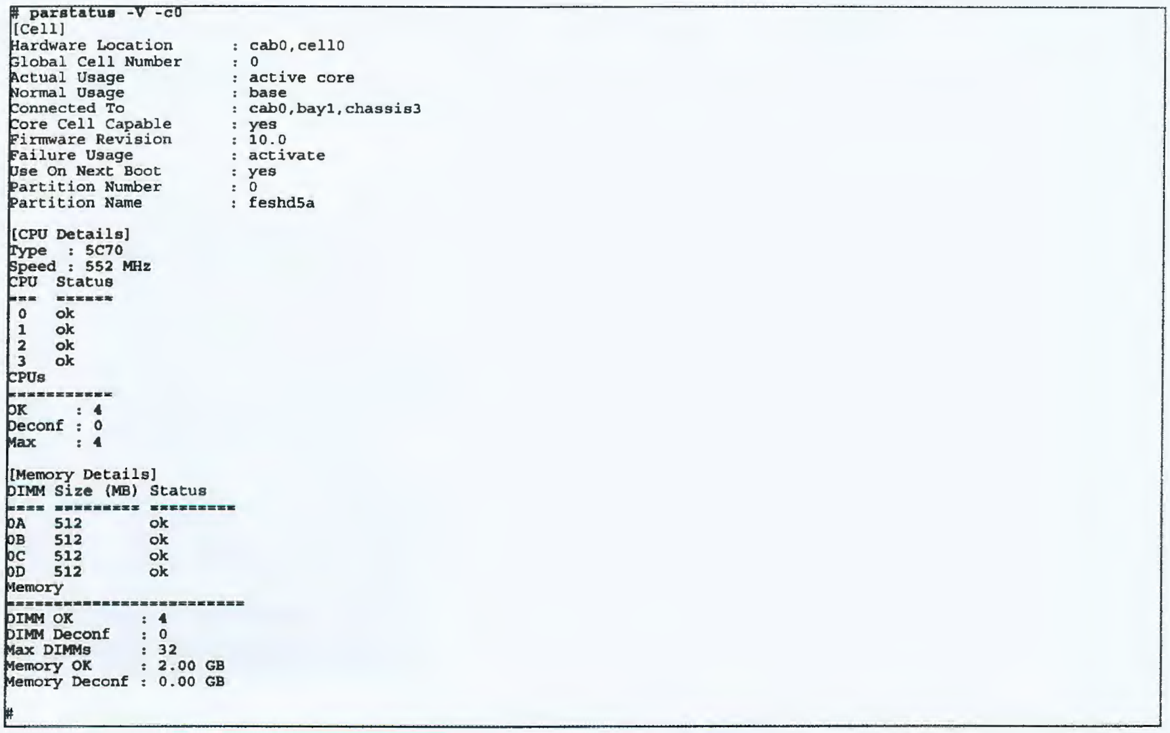
  List brief processor and memory information for all cells in the entire complex.

- **parstatus -V -p#**

  List brief processor and memory information for all cells assigned to the specified nPartition.

SU64
21

The following example shows the `parstatus -V -c0` command's output. This presents detailed processor and memory info for cell 0 in cabinet 0.



```
# parstatus -V -c0
[Cell]
Hardware Location       : cab0,cell0
Global Cell Number      : 0
Actual Usage            : active core
Normal Usage            : base
Connected To            : cab0,bay1,chassis3
Core Cell Capable       : yes
Firmware Revision       : 10.0
Failure Usage           : activate
Use On Next Boot        : yes
Partition Number        : 0
Partition Name          : feshd5a

[CPU Details]
Type  : 5C70
Speed : 552 MHz
CPU   Status
===   ======
 0    ok
 1    ok
 2    ok
 3    ok
CPUs
===========
OK     : 4
Deconf : 0
Max    : 4

[Memory Details]
DIMM Size (MB) Status
==== ========= =========
0A   512       ok
0B   512       ok
0C   512       ok
0D   512       ok
Memory
=========================
DIMM OK       : 4
DIMM Deconf   : 0
Max DIMMs     : 32
Memory OK     : 2.00 GB
Memory Deconf : 0.00 GB

#
```

Listing Cell Processors and Memory [Partition Manager]

Use the **Cell —> Show Cell Details** action, **CPUs/Memory** tab to list cell processor and memory details from Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. On the left of the primary window, select the nPartition to which the cell is assigned, or select Available Resources if the cell is unassigned.

Step 3. On the right of the primary window, select the cell whose processor and memory details you want to list, then select the **Cell —> Show Cell Details** menu item.

Step 4. Click the **CPUs/Memory** tab to list the selected cell's processor and memory configurations.

Deconfiguring Cells, Processors, and Memory

You can **deconfigure (make inactive) a cell** that is assigned to an nPartition by setting its use-on-next-boot value to "n" (do not use). This causes the cell to remain assigned to the nPartition, but the cell will be inactive the next time its nPartition boots, meaning the cell's resources will not be used.

You also can **deconfigure processors and memory** from any cell that is assigned to an nPartition. This causes the deconfigured processors or memory to not be available for use by the cell or its nPartition.

Whenever you configure or deconfigure cells, processors, or memory, *you must reboot the corresponding nPartition* for the configuration change to take effect.

You can use the following procedures:

- *Deconfiguring Cells, Processors, and Memory [BCH]* on page 337
- *Deconfiguring Cells, Processors, and Memory [HP-UX]* on page 339
- *Deconfiguring Cells, Processors, and Memory [Partition Manager]* on page 340

Deconfiguring Cells, Processors, and Memory [BCH]

Use the Configuration menu `CELLCONFIG` or `CPUCONFIG` command, or Service menu `DIMMDEALLOC` command, to configure and deconfigure cells, processors, and memory from the BCH interface.

Step 1. Access the BCH interface for the nPartition whose cells, processors, or memory you want to configure or deconfigure.

Step 2. To change *cell or processor* configurations, access the Configuration menu. To change *memory* configurations, access the Service menu.

To access the Configuration menu, enter `CO` at the BCH interface's main menu. To access the Service menu enter `SER`.

Step 3. Configure or deconfigure the cell, processors, or memory.

5461

You *cannot* deconfigure the last cell, processor, or DIMM rank. Cells must have at least one configured processor or DIMM rank, and nPartitions must have at least one configured cell.

- **Cells**

  From the Configuration menu, use the `CELLCONFIG` command to configure or deconfigure a cell in the nPartition.

  `CELLCONFIG # OFF` deconfigures the cell (#) by setting its use-on-next-boot value to "n" (do not use).

  `CELLCONFIG # ON` configures the specified cell (#) by setting its use-on-next-boot value to "y" (use the cell).

  Enter **`HELP CELLCONFIG`** for details.

- **Processors**

  From the Configuration menu, use the `CPUCONFIG` command to configure or deconfigure a processor on a cell in the nPartition.

  `CPUCONFIG` ***`cell cpu`*** **`OFF`** deconfigures the specified processor (*cpu*) on the specified cell (*`cell`*).

  `CPUCONFIG` ***`cell cpu`*** **`ON`** configures the specified processor on the cell

  Enter **`HELP CPUCONFIG`** for details.

- **Memory**

  DIMMs operate in ranks of four. Each rank is numbered (0, 1, 2, and so on) and the DIMMs in the rank are lettered (A to D). For example, rank 0 includes DIMMs 0A, 0B, 0C, and 0D.

  From the Service menu, use the `DIMMDEALLOC` command to configure or deconfigure memory on a cell in the nPartition.

  When you deallocate a DIMM, *all other DIMM's in the rank also will not be used* the next time the nPartition boots.

  `DIMMDEALLOC` ***`cell dimm`*** **`OFF`** deconfigures the specified DIMM (*dimm*) on the cell (*`cell`*) indicated.

  `DIMMDEALLOC` ***`cell dimm`*** **`ON`** configures the specified DIMM on the cell.

5460

For example, `DIMMDEALLOC 0 1B OFF` sets DIMM 1B on cell 0 to be deallocated the next time the nPartition boots, and as a result all other DIMMs in the same rank (1A, 1C, and 1D) also will not be used.

Enter **`HELP DIMMDEALLOC`** for details.

Step 4. Reboot the nPartition using the **`REBOOT`** command.

Whenever changing cell, processor, or memory configurations you must reboot the corresponding nPartition to allow the configuration changes to take place.

Deconfiguring Cells, Processors, and Memory [HP-UX]

Use the **`parmodify -p# -m#::[y|n]:`** command to configure or deconfigure (makes inactive) cells from the HP-UX command line.

Step 1. Login to HP-UX on the nPartition whose cell you want to configure or deconfigure.

Step 2. Issue the **`parstatus -C`** command to list all cells, their nPartition assignments, their actual (current) usage, and their use-on-next-boot values.

Step 3. Issue the **`parmodify -p# -m#::[y|n]:`** command to configure or deconfigure the specified cell (`-m#`) from the nPartition (`-p#`).

The **`parmodify -p# -m#::n:`** command deconfigures the specified cell (`-m#`). This sets the cell's use-on-next-boot value to "n" (do not use).

The **`parmodify -p# -m#::y:`** command configures the specified cell to be used. This sets the cell's use-on-next-boot value to "y" (use the cell).

The partition number (`-p#`) you specify must be the local nPartition number, which you can list using the `parstatus -w` command.

Step 4. Reboot the nPartition using the **`shutdown -R`** command.

You must reboot the partition to allow the new use-on-next-boot values to take effect.

The `shutdown -R` command performs a reboot for reconfig for the nPartition, which allows *all cells* to reboot, including any currently inactive cells in the nPartition.

Deconfiguring Cells, Processors, and Memory [Partition Manager]

Use the **Partition —> Modify Partition** menu, **Change Cell Attributes** tab to configure and deconfigure (makes inactive) cells using Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. Select the nPartition whose cell configuration you want to modify, then select the **Partition —> Modify Partition** menu item.

Step 3. Click the **Change Cell Attributes** tab.

Step 4. Select the cell whose configuration you want to modify, then click the **Modify Cell(s)** button.

Step 5. In the Modify Cell Attributes window, set the cell's use-on-next-boot value, then click the **OK** button.

To configure the cell to be used set use-on-next-boot to "yes".

To configure the cell *to not* be used set use-on-next-boot to "no".

Step 6. Exit Partition Manager, then reboot the corresponding nPartition using the **`shutdown -R`** command.

You must reboot the nPartition whose use-on-next-boot cell values you changed to allow the new use-on-next-boot values to take effect.

Listing the Server Product Number and Serial Number

You can list the *product number* and the *serial number* for your server complex by using software commands and utilities.

You can use the following procedures:

- *Listing Product and Serial Numbers [Service Processor]* on page 341
- *Listing Product and Serial Numbers [BCH]* on page 342
- *Listing Product and Serial Numbers [HP-UX]* on page 343
- *Listing Product and Serial Numbers [Partition Manager]* on page 343

Listing Product and Serial Numbers [Service Processor]

Use the Command menu **ID** command to list the system complex's product number and serial number from the service processor.

Step 1. Login to the system's service processor and enter **CM** to access the Command menu.

Step 2. Issue the service processor Command menu's **ID** command to display the system complex information, including the product and serial numbers.

Step 3. Type **n** (or type **q**) to *not modify* the system complex information that was displayed.

```
GSP:CM> ID

This command allows you to change certain fields in the Stable complex
configuration portion of the complex profile.

Retrieving the stable complex configuration portion of the complex profile.

    GSP modifiable stable complex configuration data fields.
    Model String           : 9000/800/SD64000
    Complex System Name    : feshd5
    Complex Serial Number  : USR2024FP1
    Original Product Number: A5201A
    Current Product Number : A5201A
    Enterprise Id          :
```

```
    Do you want to modify any of this information? (Y/[N]) n

    -> No fields modified.
GSP:CM>
```

Listing Product and Serial Numbers [BCH]

Use the Information menu **CID** command to list the system complex's product number and serial number from the BCH interface.

Step 1. Access the BCH interface for any nPartition in the complex.

You can list the complex's product number and serial number from any nPartition in the server.

Step 2. Access the BCH Information menu by entering **IN** from the BCH Main menu.

If you are at a BCH menu other than the Main menu, enter `MA` to go to the Main menu and then enter `IN` to access the Information menu.

Step 3. From the BCH Information menu, use the **CID** command to list the complex's ID information, including the product number and serial number.

The `CID` BCH command (also: `ComplexID`) displays information that is stored as part of the server's Stable Complex Configuration Data.

```
Information Menu: Enter command > CID

COMPLEX ID INFORMATION

                 Complex Name: feshd4
                 Model String: 9000/800/SD16000
      Original Product Number: A5201A
       Current Product Number: A5201A
                Serial Number: USR2025FP2
                Enterprise ID: 0x2020202020202020
    Number of Supported Cells: 32
      Complex Revision Number: 1.0

Information Menu: Enter command >
```

Listing Product and Serial Numbers [HP-UX]

Use the **parstatus -X** command to list a system complex's product number and its serial number from HP-UX.

Step 1. Login to HP-UX running on any of the system's nPartitions.

You can list the product and serial numbers from any nPartition.

Step 2. Issue the **parstatus -X** command and option to display system complex attributes, including the product and serial numbers.

```
# parstatus -X
[Complex]
   Complex Name : feshd5
   Complex Capacity
     Compute Cabinet (8 cell capable) : 2
     IO Expansion Cabinet             : 1
   Active GSP Location : cabinet 0
   Model : 9000/800/SD64000
   Serial Number : USR2024FP1
   Current Product Number : A5201A
   Original Product Number : A5201A
   Complex Profile Revision : 1.0
   The total number of Partitions Present : 2

#
```

Listing Product and Serial Numbers [Partition Manager]

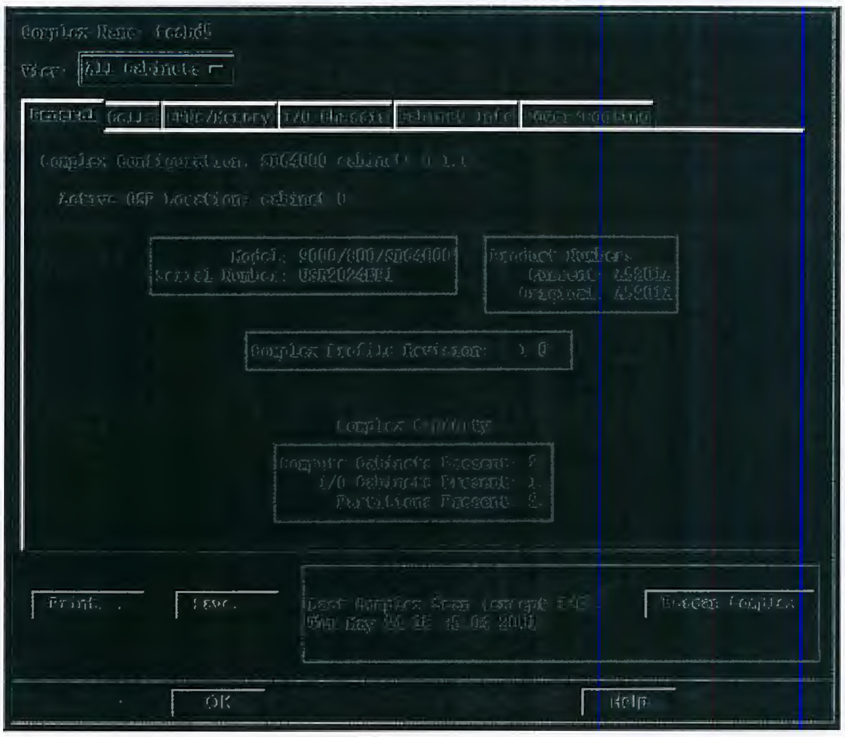
Use the **Complex —> Show Complex Details** menu to list the system complex's product and serial numbers using Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. Select the **Complex —> Show Complex Details** menu item.

The Complex Details window displays the complex's product and serial numbers through the **General** tab.

S455



Complex Name: feshd5

View: All Cabinets

Complex Configuration: SD64000 cabinet 0 1 1

Active GSP Location: cabinet 0

Model: 9000/800/SD64000
Serial Number: USR2024FB1

Product Numbers:
Current: A5201A
Original: A5201A

Complex Profile Revision: 1.0

Complex Capacity

Compute Cabinets Present: 2
I/O Cabinets Present: 1
Partitions Present: 2

Last Complex Scan (except I/O):
Tue May 01 16:45:02 2001

5454

Checking Blower and Fan Status

You can remotely check the operating status of a server complex's blowers and fans by using software commands and utilities.

NOTE Different HP server and cabinet models have different blower and fan configurations.

You can use the following procedures:

- *Checking Fan Status [Service Processor]* on page 345
- *Checking Fan Status [HP-UX]* on page 346
- *Checking Fan Status [Partition Manager]* on page 347

Checking Fan Status [Service Processor]

Use the `PS` command's "Cabinet" option to check fan and blower status from the service processor Command menu.

Step 1. Login to the complex's service processor and enter `CM` to access the Command menu.

Step 2. Issue the `PS` command, select the "Cabinet" option, and specify the cabinet number whose fan status you want to check.

SYS2
21

```
Fan 3  ok

I/O Fans
=============
Fan 0  ok
Fan 1  failed
Fan 2  ok
Fan 3  ok
Fan 4  ok

Bulk Power Supplies(BPS)
=======================
Power Supply  0  ok
...
```

Checking Fan Status [Partition Manager]

Use the **Complex —> Show Complex Details** menu, **Power/Cooling** tab to list fan status from Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. Select the **Complex —> Show Complex Details** menu item.

This displays the Complex Details window.

Step 3. Click the **Power/Cooling** tab to view the panel that has information about the status of the blowers and fans in the complex.

SUS1

Complex Health Analysis of a Server

You can quickly check for hardware problems in an nPartition server by using Partition Manager's "Analyze Complex Health" feature.

This feature scans the server complex and uses problem detectors to check the operating status of cells, I/O chassis, fans and blowers, and power supplies.

Partition Manager automatically performs this task when you launch the application; if any problems are detected then the complex health analysis is displayed before Partition Manager's primary window.

Analyzing Server Complex Health [Partition Manager]

Use the **Complex —> Analyze Complex Health** action to quickly check a server complex's operating status from Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. Select the **Complex —> Analyze Complex Health** action.

Partition Manager displays a window that reports the hardware analysis results. To re-analyze the server's health click the **Refresh** button.

5449

Listing the Cabinets in a Server Complex

You can list all cabinets in a server complex by using software commands and utilities, which allow you to determine the complex's cabinet configuration from a remote location.

You can use the following procedures:

- *Listing Cabinets [Service Processor]* on page 350
- *Listing Cabinets [HP-UX]* on page 351
- *Listing Cabinets [Partition Manager]* on page 351

Listing Cabinets [Service Processor]

Use the Command menu DU command to list all cabinets in the server complex using the service processor.

Step 1. Login to the server's service processor and enter CM to access the Command menu.

Step 2. Issue the DU command to list all cabinets in the server complex.

```
GSP:CM> DU

The following GSP bus devices were found:
+----+-----+-----------+----------------+-----------------------------------+
|    |     |           |                |             Core IOs              |
|    |     |           |                | IO Bay | IO Bay | IO Bay | IO Bay |
|    |     |   UGUY    |     Cells      |    0   |    1   |    2   |   3    |
|Cab.|     |           |                |IO Chas.|IO Chas.|IO Chas.|IO Chas.|
| #  | GSP | CLU | PM  |0 1 2 3 4 5 6 7 |0 1 2 3 |0 1 2 3 |0 1 2 3 |0 1 2 3 |
+----+-----+-----+-----+----------------+--------+--------+--------+--------+
|  0 |  *  |  *  |  *  |*   *   *   *   |      * |      * |        |        |
|  1 |     |  *  |  *  |*   *   *       |        |      * |        |        |
|  8 |     |  *  |  *  |                |      * |  *     |        |        |

GSP:CM>
```

5448

Listing Cabinets [HP-UX]

Use the **parstatus -B** or **parstatus -V -b#** command to list cabinet details from HP-UX.

Step 1. Login to HP-UX running on any of the server's nPartitions.

You can list cabinet information from any nPartition.

Step 2. Issue the **parstatus -B** command and option to list all cabinets and their current status.

For more information, issue the **parstatus -V -b#** command for details on the specified cabinet number (-b#).

```
# parstatus -B
[Cabinet]
                   Cabinet    I/O        Bulk Power  Backplane
                   Blowers    Fans       Supplies    Power Boards
                   OK/        OK/        OK/         OK/
Cab                Failed/    Failed/    Failed/     Failed/
Num Cabinet Type N Status   N Status   N Status    N Status       GSP
=== ============ ========= ========= ========== ============    ======
 0   SD64000       4/ 0/ N+  5/ 0/ ?    5/ 0/ N+     3/ 0/ N+      active
 1   SD64000       4/ 0/ N+  5/ 0/ ?    5/ 0/ N+     3/ 0/ N+      none

Notes: N+ = There are one or more spare items (fans/power supplies).
       N  = The number of items meets but does not exceed the need.
       N- = There are insufficient items to meet the need.
       ?  = The adequacy of the cooling system/power supplies is unknown.

#
```

Listing Cabinets [Partition Manager]

Use the **Complex —> Show Complex Details** menu, **Cabinet Info** panel to list the cabinets in a server complex from Partition Manager.

Step 1. Run Partition Manager (/opt/parmgr/bin/parmgr) or access it from SAM or a Web browser.

Step 2. Select the **Complex —> Show Complex Details** menu item, then click the **Cabinet Info** panel.

5487

Listing the nPartitions in a Server

You can list details about the nPartitions defined in a server complex, including the partition numbers, nPartition names, and the cells assigned to the nPartitions.

You can use the following procedures:

- *Listing nPartitions [Service Processor]* on page 352
- *Listing nPartitions [HP-UX]* on page 353
- *Listing nPartitions [Partition Manager]* on page 353

Listing nPartitions [Service Processor]

Use the Command menu **CP** command to list all nPartitions from the service processor.

Step 1. Login to the server's service processor and enter **CM** to access the Command menu.

Step 2. Issue the service processor Command menu's **CP** command to list all nPartitions defined in the server complex.

The CP command lists the partition number (Part 0, Part 1, and so on) for each nPartition and lists which cells are assigned to each nPartition.

```
GSP:CM> CP

--------------
Cabinet | 0  |
--------+----+
 Slot   |0123|
--------+----+
Part  0 |*...|
Part  1 |.*..|

GSP:CM>
```

5446

Listing nPartitions [HP-UX]

Use the **parstatus -P** command to list a server's nPartitions from HP-UX.

Step 1. Login to HP-UX running on any of the server's nPartitions.

You can list all nPartitions from any nPartition in the server.

Step 2. Issue the **parstatus -P** command and option to list all nPartitions and their current status.

```
# parstatus -P
[Partition]
Par                 # of  # of I/O
Num Status          Cells Chassis  Core cell  Partition Name (first 30 chars)
=== ============ ===== ======== ========== ===============================
 0  active          2       2      cab0,cell0 jules00
 1  active          2       2      cab0,cell4 jules01
#
```

Listing nPartitions [Partition Manager]

View the left side of the primary window to see a display of all nPartitions in the server from Partition Manager.

Step 1. Run Partition Manager (/opt/parmgr/bin/parmgr) or access it from SAM or a Web browser.

Step 2. Access Partition Manager's primary window, and view the list of nPartitions shown on the window's left side.

Each nPartition is listed separately. Also listed here are the server's Available Resources, which are not assigned to any nPartition.

5445

Naming or Renaming a Server Complex

You can assign a name for each server complex in order to better identify the complex as you work with it.

Several commands and utilities display the server complex name as part of their output and interfaces. For example, some nPartition commands and Partition Manager list the complex name.

The server complex name only serves as a helpful identifier; changing the name does not affect the way in which commands and utilities interact with the complex.

You can use the following procedures:

- *Renaming a Server Complex [Service Processor]* on page 354
- *Renaming a Server Complex [Partition Manager]* on page 355

The server complex name is stored as part of the server's complex profile (part of its "stable complex configuration" data).

NOTE Each server complex name has up to 20 characters, which can include upper- and lowercase letters; numbers; and dashes, underscores, periods, and spaces (“-” “_” “.” and “ ”).

Renaming a Server Complex [Service Processor]

Use the Command menu `ID` command to list and modify the server complex name from the service processor.

Step 1. Login to the server's service processor and enter `CM` to access the Command menu.

Step 2. Issue the service processor Command menu's `ID` command to list the complex's name.

The `ID` command lists some of the current server complex's "stable complex configuration" data, including the complex name.

```
GSP:CM> ID

This command allows you to change certain fields in the Stable complex
configuration portion of the complex profile.

Retrieving the stable complex configuration portion of the complex profile.

    GSP modifiable stable complex configuration data fields.
    Model String             : 9000/800/SD64000
    Complex System Name      : feshd5
    Complex Serial Number    : USR2024FP1
    Original Product Number: A5201A
    Current Product Number : A5201A
    Enterprise Id            :

    Do you want to modify any of this information? (Y/[N])
```

Step 3. Specify whether you want to modify the complex profile, including its name.

You should only modify the “complex system name”. Do not change the model string, serial number, or other details used by commands, utilities, and licensing tools.

To cancel the changes at any time, enter **q** to quit the `ID` command without modifying the complex profile data.

Renaming a Server Complex [Partition Manager]

Use the **Complex —> Set Complex Name** action to rename a server complex using Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web interface.

Step 2. Select the **Complex —> Set Complex Name** menu item.

Step 3. Enter the complex’s new name in the pop-up window.

The pop-up window shows the current complex name. If no name was previously assigned, the default name is “MyComplex”.

Step 4. Click **OK** to set the new name or click **Cancel** to keep the previously assigned name.

S4U3

Checking for Power Supply Failures

From remote locations, you can check the operating status of power supplies by using software commands and utilities.

Different HP server and cabinet models have different supply requirements and configurations.

You can use the following procedures:

- *Checking Power Supply Status [Service Processor]* on page 356
- *Checking Power Supply Status [HP-UX]* on page 356
- *Checking Power Supply Status [Partition Manager]* on page 358

Checking Power Supply Status [Service Processor]

Use the Command menu **PS** command's "Cabinet" option to check power status from the service processor.

Step 1. Login to the complex's service processor and enter **CM** to access the Command menu.

Step 2. Issue the **PS** command, select the "Cabinet" option, and specify the cabinet number whose power status you want to check.

Checking Power Supply Status [HP-UX]

Use the `parstatus -B` or `parstatus -V -b#` command to list the status of power supplies from HP-UX.

Step 1. Login to HP-UX running on any of the system's nPartitions.

You can check power details from HP-UX running on any nPartition.

Step 2. Issue the `parstatus -B` command for a brief summary of all cabinets including power status, or issue the `parstatus -V -b#` command for detailed power status for a specific cabinet (`-b#`) whose details you want to view.

S442

- The `parstatus -B` command summarizes the power status for all cabinets in the system complex.
- The `parstatus -V -b#` command displays a detailed status (“ok” or “failed”) for all power supplies in the specified cabinet (`-b#`).

The following example shows power supply details for cabinet number 0, which has one failed bulk power supply (Power Supply 3).

```
# parstatus -V -b0
[Cabinet]
                 Cabinet   I/O       Bulk Power  Backplane
                 Blowers   Fans      Supplies    Power Boards
                 OK/       OK/       OK/         OK/
Cab              Failed/   Failed/   Failed/     Failed/
Num Cabinet Type N Status  N Status  N Status    N Status      GSP
=== ============ ========= ========= ==========  ============  ======
 0  SD32000       4/ 0/ N+  5/ 0/ ?   3/ 1/ N     3/ 0/ N+     active

Cabinet Blowers
===============
Fan 0  ok
Fan 1  ok
Fan 2  ok
Fan 3  ok

I/O Fans
==============
Fan 0  ok
Fan 1  ok
Fan 2  ok
Fan 3  ok
Fan 4  ok

Bulk Power Supplies(BPS)
========================
Power Supply  0  ok
Power Supply  1  ok
Power Supply  3  failed
Power Supply  4  ok

Backplane Power Boards
======================
Power Supply  0  ok
Power Supply  1  ok
Power Supply  2  ok

Notes: N+ = There are one or more spare items (fans/power supplies).
       N  = The number of items meets but does not exceed the need.
```

```
N- = There are insufficient items to meet the need.
?  = The adequacy of the cooling system/power supplies is unknown.

#
```

Checking Power Supply Status [Partition Manager]

Use the **Complex —> Show Complex Details** action, **Power/Cooling** tab to list power status from Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. Select the **Complex —> Show Complex Details** menu item.

This displays the Complex Details window.

Step 3. Click the **Power/Cooling** tab to bring up the panel that contains information about the status of the power supplies in the complex.

5440

Checking for Memory DIMM Failures

You can list cell memory configurations and check for memory DIMM failures using software tools and utilities.

You can use the following procedures:

- *Checking Memory Status [HP-UX]* on page 359
- *Checking Memory Status [Partition Manager]* on page 361

Checking Memory Status [HP-UX]

Use the **parstatus -V -c#** command to list a cell's memory status, including any DIMM failures, from HP-UX.

Step 1. Login to HP-UX running on any of the system's nPartitions.

You can check memory details for any cell from any nPartition.

Step 2. Issue the **parstatus -V -c#** command to list detailed information about the specified cell (-c#).

The detailed information parstatus reports includes a list of all DIMMs (memory modules) installed on the cell, and the status of each DIMM.

Any memory listed as "failed" either has failed self-tests or has been software deconfigured by the Boot Console Handler (BCH) Service menu's DIMMDEALLOC command.

NOTE For any DIMM that fails or is deallocated, *all other DIMMs in the same rank also are deallocated*. All four DIMMs within the same rank must pass self-test and must be allocated for the rank to be made available for use by the cell and its nPartition.

In the following example, eight DIMMs (0A–0D and 1A–1D) are installed and are available ("ok") for use by the cell's nPartition.

```
# parstatus -V -c0
[Cell]
Hardware Location        : cab0,cell0
```

SU39

```
Global Cell Number      : 0
Actual Usage            : active core
Normal Usage            : base
Connected To            : cab0,bay0,chassis1

....

[CPU Details]
Type  : 5E70
Speed : 750 MHz
CPU  Status
===  ======
 0   ok
 1   ok
 2   ok
 3   ok
CPUs
===========
OK      : 4
Deconf  : 0
Max     : 4

[Memory Details]
DIMM Size (MB) Status
==== ========= =========
0A   512       ok
0B   512       ok
0C   512       ok
0D   512       ok
1A   512       ok
1B   512       ok
1C   512       ok
1D   512       ok
Memory
=========================
DIMM OK         : 8
DIMM Deconf     : 0
Max DIMMs       : 32
Memory OK       : 4.00 GB
Memory Deconf   : 0.00 GB

#
```

In the above example, if any DIMM had failed its status would be “failed” and all other DIMMs in its rank (for instance, rank 0 or rank 1) also would be listed as failed.

5438

Any one or more of the failed DIMMs might have been software deallocated or might have failed self tests. In either case, all DIMMs in the rank automatically are deallocated when any of the rank's DIMMs fails or is deallocated.

Checking Memory Status [Partition Manager]

Use the **Cell —> Show Cell Details** action, **CPUs/Memory** tab to list a cell's memory status, including any DIMM failures, from Partition Manager.

Step 1. Run Partition Manager (/opt/parmgr/bin/parmgr) or access it from SAM or a Web browser.

Step 2. On the left of the primary window, select the nPartition to which the cell is assigned, or select Available Resources if the cell is unassigned.

Step 3. On the right of the primary window, select the cell whose memory details you want to list, then select the **Cell —> Show Cell Details** menu item.

Step 4. Click the **CPUs/Memory** tab to display the status of memory modules (DIMMs) for the cell.

5437

Checking for Processor Failures

You can list cell processor configuration, including any processor failures, using software tools and utilities.

You can use the following procedures:

- *Checking Processor Status [HP-UX]* on page 362
- *Checking Processor Status [Partition Manager]* on page 363

Checking Processor Status [HP-UX]

Use the **`parstatus -V -c#`** command to list a cell's processor status, including any failures, from HP-UX.

Step 1. Login to HP-UX running on any of the system's nPartitions.

You can check processor details for any cell from any nPartition.

Step 2. Issue the **`parstatus -V -c#`** command to list detailed information about the specified cell (`-c#`).

The detailed information `parstatus` reports includes a list of all processors (CPUs) installed on the cell, and the status of each CPU.

Any processors listed as "failed" either have failed self-tests or have been software deconfigured by the Boot Console Handler (BCH) Configuration menu's `CPUCONFIG` command.

```
# parstatus -V -c5
[Cell]
Hardware location        : cab0,cell5
Global Cell Number       : 5
Actual Usage             : active base
Normal Usage             : base
Connected To             : -
Core Cell Capable        : no
Firmware Revision        : 32.5
Failure Usage            : activate
Use On Next Boot         : yes
Partition Number         : 0
Partition Name           : betty
```

5436

```
[CPU Details]
Type  : 23664
Speed : 552 MHz
CPU  Status
===  ======
 0   ok
 1   failed
 2   ok
 3   failed
CPUs
===========
OK      : 2
Failed  : 2
Max     : 4

....
```

Checking Processor Status [Partition Manager]

Use the **Cell —> Show Cell Details** menu, **CPUs/Memory** tab to list processor details and any failures using Partition Manager.

Step 1. Run Partition Manager (`/opt/parmgr/bin/parmgr`) or access it from SAM or a Web browser.

Step 2. On the left of the primary window, select the nPartition to which the cell is assigned, or select Available Resources if the cell is unassigned.

Step 3. On the right of the primary window, select the cell whose processor details you want to list, then select the **Cell —> Show Cell Details** menu item.

Step 4. Click the **CPUs/Memory** tab to display the processors installed in the selected cell and list the status for each processor.

5435

S434

8 Online Add and Replacement (OLAR) of PCI Cards

This chapter presents background information and procedures for performing PCI I/O card *online addition and replacement* (OLAR) on HP's nPartition servers.

The main procedures for adding and replacing PCI cards are:

- *Online Addition (OLA) for a PCI Card* on page 383
- *Online Replacement (OLR) for a PCI Card* on page 389

See the sections that follow for info on tools, requirements, limitations, and other PCI card OLAR details.

For an introduction to I/O hardware on nPartition servers, refer to the chapter *nPartition System Overviews* on page 31.

Also refer to the book *Configuring HP-UX for Peripherals* for further details on configuring PCI cards and related devices.

Overview of PCI Card Online Addition and Replacement (OLAR)

HP-UX 11i supports online addition and replacement (OLAR) of PCI I/O cards on HP nPartition systems. *Without rebooting* HP-UX running on an nPartition, you can add or replace PCI cards whose device drivers support OLAR.

The HP-UX PCI card OLAR features allow for:

- *Adding a new PCI card* without affecting other components of the system and *without* requiring a system reboot.

  This procedure is presented in *Online Addition (OLA) for a PCI Card* on page 383.

- *Replacing an existing PCI card* without affecting other components of the system and *without* requiring a system reboot.

  This procedure is presented in *Online Replacement (OLR) for a PCI Card* on page 389.

nPartition System OLAR Notes

The core I/O cards in HP nPartition servers are *not supported* for online addition or replacement.

On HP rp7405/rp7410 servers, two PCI card slots (chassis 0, slot 1 and chassis 1, slot 8) are dedicated for use by a combination SCSI/LAN card. This SCSI/LAN card is supported for online addition or replacement.

On HP rp7405/rp7410 and rp8400 servers, the PCI card slot latches must be used in conjunction with PCI card OLAR procedures when HP-UX is running. When a card slot latch is open, the slot is powered off and the slot is made accessible for card addition or replacement.

See the chapter *nPartition System Overviews* on page 31 and the section *PCI Card Slot Latches and Doorbells* on page 376 for other I/O hardware details.

5432

OLAR Tools and Interfaces

This section discusses the tools available for performing online card addition and replacement tasks. Also given here are example uses of some of the commonly used OLAR commands and interfaces.

The primary tools for performing PCI card OLAR tasks are the System Administration Manager utility (SAM, `/usr/sbin/sam`) and Partition Manager (`/opt/parmgr/bin/parmgr`).

NOTE Always use SAM or Partition Manager when performing card addition and replacement tasks, because these tools perform critical resource analysis and properly execute all scripts and commands in the correct sequences.

The `/usr/bin/rad` command and other utilities also can provide useful OLAR-related information.

Details on the OLAR tools and interfaces are given in Table 8-1.

Table 8-1 Tools and Interfaces for PCI Card Online Addition and Replacement (OLAR)

OLAR Tool/Interface	Description
System Administration Manager (SAM)	`/usr/sbin/sam` SAM provides both a graphical user interface (GUI) and an equivalent text-based terminal interface. To perform OLAR tasks from SAM, enter the **Peripheral Devices > Cards** area, which gives a listing of all PCI cards currently available in the local nPartition. When you select a slot or path from this list, items in the **Actions** menu enable you to perform OLAR-related tasks on the selection.

SU31

Table 8-1 **Tools and Interfaces for PCI Card Online Addition and Replacement (OLAR) (Continued)**

OLAR Tool/Interface	Description
Partition Manager	`/opt/parmgr/bin/parmgr` Partition Manager's interface is exclusively a GUI. In addition to supporting nPartition administration tasks, Partition Manager has complete support for PCI card OLAR. To perform OLAR tasks from Partition Manager, select and "open" an I/O chassis in the primary window, which gives a listing of all PCI cards in the selected I/O chassis. When you select a slot or path from this list, items in the **I/O** menu enable you to perform OLAR-related tasks on the selection. Note that when using Partition Manager you can add or replace cards in the *local* nPartition's active I/O chassis only.
`/usr/bin/rad`	The `rad` command is a command-line interface for performing some OLAR tasks and getting system PCI card and driver status information for the local nPartition. HP recommends you perform online card add or replace tasks using SAM or Partition Manager—not `rad`. However, the `rad` command can be useful for listing status, getting additional slot or card details, and for independently managing card slot attention indicators (LEDs). The `rad` command reports *the default speed/frequency* for PCI slots when they are not occupied. When a slot is occupied with a card the `rad` command reports *the operating speed/frequency* for the card and slot. See *Example Uses of Common rad Commands* on page 370 for other details.

S430

Table 8-1 Tools and Interfaces for PCI Card Online Addition and Replacement (OLAR) (Continued)

OLAR Tool/Interface	Description
Scripts in the directory `/usr/sbin/olrad.d/`	Each OLAR-capable card's driver(s) may have associated scripts in the `/usr/sbin/olrad.d/` directory. Each driver's script accepts the following command-line arguments: the *`action`* to perform and *`path`* for the slot for which the action is performed. The SAM and Partition Manager utilities automatically run these scripts, as needed, when performing PCI card online addition or replacement tasks. Normally, the driver OLAR scripts *are not invoked manually* by administrators. These scripts' actions include various preface–, prepare–, and post-replace tasks and post-add tasks.
I/O Chassis Hardware	Hardware in each I/O chassis includes PCI card slots, card slot dividers, and power and attention indicators (LEDs) for each slot. HP rp7405/rp7410 and rp8400 servers also have PCI card slot latches. Note that the I/O chassis locations and other features of I/O chassis hardware differ in the various HP nPartition server models. Refer to the chapter *nPartition System Overviews* on page 31 and the section *PCI Card Slot Latches and Doorbells* on page 376 for nPartition I/O hardware details.
`/usr/lib/libolrad.1`	The `libolrad` library is used by the `rad` command and other utilities such as SAM and Partition Manager to support PCI card slot inquiry and online addition and replacement tasks.

5429

Example Uses of Common rad Commands

This section gives summaries and examples uses of common `rad` commands and options.

Table 8-2 **rad Command Commonly Used Options**

Command	Description
`rad -q`	Displays the status of all OLAR-capable slots in the *local* nPartition. Only displays slots in currently active I/O chassis.
`rad -N` *`path`*	Lists the slot ID for the specified hardware path (*`path`*). The `rad -N` command gives info for OLAR-capable slots only.
`rad -f` *`flag slot`*	Sets the attention indicator (LED) for the specified slot. The accepted *`flag`* arguments: on, `attention`, and `off`, where `attention` flashes the specified slot's LED, and on and `off` turn the LED steady-on or off.
`rad -c` *`slot`*	Displays the device information for all functions/interfaces at the specified slot.

See the *rad* (1M) manpage for complete details.

Example 8-1 **Commonly Used rad Commands for nPartition I/O Details and Card Add/Replace Tasks**

- **`rad -q`**

  To list basic slot, path, card, and driver details, use the `rad -q` command.

  The `rad -q` command lists all PCI card slots in the local nPartition, the corresponding hardware paths, and the current status of all slots and drivers.

```
# rad -q
                                                                    Driver(s)
Slot        Path        Bus   Speed   Power   Occupied    Suspended  Capable
0-0-0-1     0/0/8/0     64    33      On      No          N/A        N/A
0-0-0-2     0/0/10/0    80    33      On      No          N/A        N/A
0-0-0-3     0/0/12/0    96    33      On      Yes         No         Yes
0-0-0-4     0/0/14/0    112   33      On      No          N/A        N/A
0-0-0-5     0/0/6/0     48    33      On      Yes         Yes        Yes
0-0-0-6     0/0/4/0     32    33      On      No          N/A        N/A
```

5428

```
0-0-0-7      0/0/2/0      16     33      On      No        N/A        N/A
0-0-0-8      0/0/1/0      8      33      On      No        N/A        N/A
#
```

- **`rad -N`** ***`path`***

  To determine which card slot corresponds to a hardware path, use the `rad -N` *`path`* command.

  The `rad -N` *`path`* command lists the card slot used by the device whose hardware path you specify. The slot is reported in *cabinet-bay-chassis-slot* format.

```
# rad -N 0/0/6/0/0.6.0
0-1-3-5
#
```

- **`rad -f`** ***`flag slot`***

  To flash, turn on, or turn off a PCI slot's attention indicator (LED) use the `rad -f` *`flag slot`* command.

```
# rad -f attention 0-1-3-1
# rad -f off 0-1-3-1
#
```

- **`rad -c`** ***`slot`***

  To list device information about a card use the `rad -c` *`slot`* command.

  The `rad -c` *`slot`* command lists details for all interfaces in a card, including the hardware path(s), driver name(s), and vendor and revision details.

```
# rad -c 0-1-3-5
Path                   :0/0/6/0/0
Name                   :c720
Device_ID              :000f
Vendor_ID              :1000
Subsystem_ID           :0000
Subsystem_Vendor_ID    :0000
Revision_ID            :4
Class                  :010000
Status                 :0200
Command                :0156
Multi_func             :No
Bridge                 :No
Capable_66Mhz          :No
Power_Consumption      :75

#
```

S427

Requirements for OLAR Operations

To perform a card *addition* or card *removal-and-replacement* operation, the following system requirements must be met:

- The add or replace operation **must** be supported on the system hardware.

  All HP nPartition servers support PCI card OLAR.

- The replacement PCI card **must** be identical to the original card.

  When performing a card replacement task, you must use a replacement card that: uses the *same driver*, is manufactured by the *same vendor*, and is the *same hardware revision* as the original card being replaced.

  Use the `rad -c` *`slot`* command to list detailed driver, vendor, and revision information for a card in the specified slot.

- The PCI card's driver **must** support OLAR.

  Some PCI card drivers do not support OLAR.

  Use the `rad -q` command's output to check whether an existing PCI card's driver is capable of being suspended and resumed for card OLAR operations.

  Both SAM and Partition Manager also indicate in the "Status" column whether an existing PCI card's driver supports OLAR. All card slots except those listed as "not OLAR-able" are valid for online PCI card add or replace tasks.

- The card's driver **must** be loaded in the currently running HP-UX kernel.

  For online *addition*, the driver must be present in the kernel to support the new card.

  For online *replacement*, the replacement card must use the same revision of the driver as the original card.

  Use the SAM utility's **Kernel Configuration > Drivers** area to list all currently loaded drivers.

- The PCI slot **must** have firmware that supports OLAR.

  On all HP nPartition servers, the I/O firmware supports OLAR.

5426

- The card **must** fit into the slot.

  On all nPartition servers, all PCI card slots can accept PCI cards keyed as universal cards.

  However, in nPartition server I/O chassis the PCI card slots also are physically keyed to accept cards that either are keyed as 5-volt cards or keyed as 3.3-volt cards.

  See the chapter *nPartition System Overviews* on page 31 for details on I/O slot capabilities.

- The resources supported by the card **must not** be critical for the server's continued operation.

  Resources that do not have a defined failover are considered to be "critical resources" that cannot be replaced online.

  For example, the following cards may be considered critical resources: cards that connect to disks for active filesystems, or a LAN card that provides the network port used by the current instance of SAM.

  You could replace a SCSI card used by a disk with an active filesystem, if the filesystem were mirrored on a different disk supported by a second SCSI card. In this case LVM could automatically failover to the mirrored disk, thus allowing you to perform an online replacement of the original SCSI card.

NOTE The core I/O cards on HP nPartition servers *are not* supported for online addition or replacement (OLAR) operations.

5425

PCI Card OLAR Considerations

This section discusses two issues of possible concern when performing PCI card OLAR tasks: card slot power domains, and multi-function cards.

Power Domains

Each **power domain** consists of all the PCI card slots that are powered on or off together as a unit.

On HP nPartition servers *each slot is in its own power domain*, which allows each slot to power on or off without affecting any other slots.

Both SAM's and Partition Manager's OLAR procedures automatically check the effects of OLAR operations on the slots in a power domain. However, in all nPartition servers each slot's power is independent.

To list all slots in a power domain, use the **`rad -a`** ***`slot`*** command. For example, the following `rad` command output indicates that slot 0-1-3-5 is in its own power domain.

```
# rad -a 0-1-3-5
0-1-3-5
#
```

Multi-Function Cards

A **multi-function card** provides more than one function in a single PCI card that occupies one slot. For example: a dual-SCSI PCI card has two SCSI ports, and a combination SCSI/LAN PCI card has both a SCSI port and a LAN port. Such cards allow a single PCI card slot to provide services that otherwise would require two or more PCI cards.

A multi-function card has a separate hardware path for each function, and has a separate driver bound at each hardware path.

Both SAM's and Partition Manager's OLAR procedures automatically check for critical resources at all hardware paths of multi-function cards. These utilities also suspend and resume all drivers bound to multi-function cards as required for OLAR purposes.

To list all functions provided by a PCI card slot, use the **rad -h** ***slot*** command. For example, the following rad command lists all hardware paths associated with slot 0-1-3-8 (cabinet 0, bay 1, chassis 3, slot 8).

```
# rad -h 0-1-3-8
0/0/11/0/0
0/0/11/0/1
#
```

As the above example shows, slot 0-1-3-8 has two functions, one at each of the hardware paths listed.

To list all drivers bound to a multi-function card, use the **rad -c** ***slot*** command.

To list additional details about a multi-function card, use the **ioscan -H** ***path*** command and specify only the first three fields (*cell/SBA/LBA*) of the card's hardware path.

On HP nPartition servers, each card slot has its own local bus adapter (LBA) that is shared by all ports on the card that occupies the slot. For example, the following ioscan command lists two SCSI ports that are provided by the card at hardware path 0/0/11.

```
# ioscan -H 0/0/11
H/W Path        Class                       Description
=======================================================
0/0/11                 ba                   Local PCI Bus Adapter (782)
0/0/11/0/0                    ext_bus       SCSI C896 Ultra2 Wide LVD
0/0/11/0/0.7                     target
0/0/11/0/0.7.0                      ctl     Initiator
0/0/11/0/1                    ext_bus       SCSI C896 Ultra2 Wide LVD
0/0/11/0/1.7                     target
0/0/11/0/1.7.0                      ctl     Initiator
#
```

PCI Card Slot Latches and Doorbells

NOTE This section applies only to HP rp7405/rp7410 and rp8400 servers.

This section introduces two features of HP rp7405/rp7410 and rp8400 server I/O chassis: PCI card slot latches and PCI card slot doorbell buttons.

PCI Card Slot Latches

Both HP rp7405/rp7410 and rp8400 servers have slot latches for all PCI card slots; each PCI card slot has its own latch.

Each PCI card slot latch can enable or disable power to its card slot and, when closed, the latch can secure a PCI card in place. These slot latches are accessible when you have removed the top cover from an HP rp7405/rp7410 or rp8400 server chassis.

Card slot latches are used both for *offline* PCI card procedures and for *online* PCI card procedures.

When a PCI slot latch is open, the slot is powered off.

When a PCI slot latch is closed, the slot can have power enabled. However, note that when a slot's latch is closed the slot's power can be disabled as part of a PCI card OLAR procedure from SAM or Partition Manager, or as a manual operation performed from the HP-UX command-line or from a service processor (GSP or MP) command.

NOTE When HP-UX is running in the nPartition to which an I/O chassis belongs, you should use SAM or Partition Manager procedures to prepare a PCI card slot before opening or closing the slot's latch.

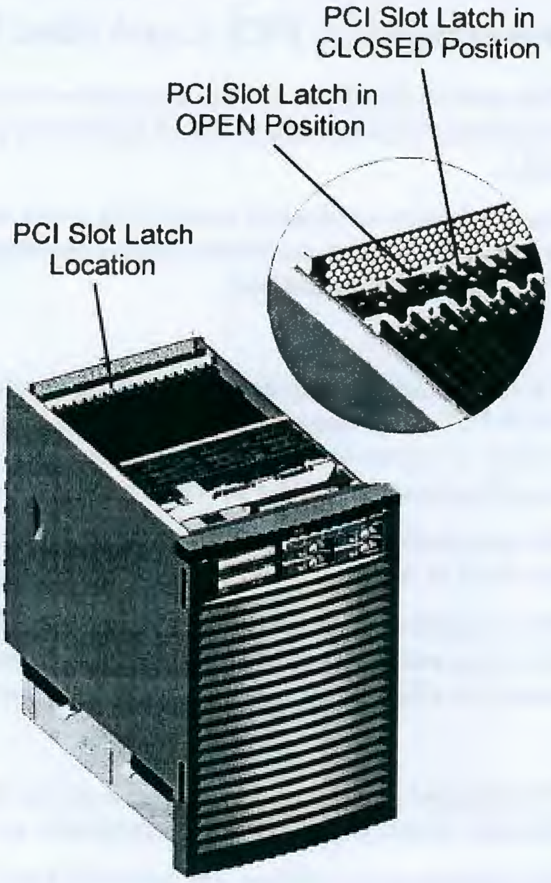
Otherwise you may encounter unpredictable results.

Figure 8-1 on page 377 shows positions of PCI card slot latches. While an HP rp8400 server is shown in Figure 8-1, HP rp7405/rp7410 card slot latches are available in the same location and operate identically.

5422

21

Figure 8-1 **PCI Card Slot Latches (HP rp7405/rp7410 and rp8400)**


PCI Slot Latch in CLOSED Position
PCI Slot Latch in OPEN Position
PCI Slot Latch Location

PCI Card Slot "Doorbells"

NOTE

This section applies only to HP rp7405/rp7410 and rp8400 servers.

The "doorbell" buttons currently have no functions. Pressing a card slot doorbell button has no impact on system operations.

On both HP rp7405/rp7410 and rp8400 servers, access to the doorbell buttons is prevented by a plastic covering.

The PCI card slot doorbell buttons are provided for future expanded functionality.

5421

21

Determining PCI Card Slot Locations

This section describes how to determine which PCI card slot is used by a filesystem, network interface, or hardware path (such as a boot device path).

You may want to identify which PCI cards are used by critical and non-critical system resources when planning for card replacement or nPartition reconfiguration.

NOTE While you can use the manual techniques described here to help identify which PCI cards support critical system resources, you should rely on the critical resource analysis that SAM and Partition Manager perform for a complete analysis of the services a card provides.

You can perform SAM or Partition Manager critical resource analysis for any card in an nPartition's active I/O chassis.

When performing a *card replacement* action, both SAM and Partition Manager automatically check for any critical system resources that would be affected by taking the card offline.

The manual procedures described here use the `rad -N` *`path`* command to identify which PCI card slot corresponds to the specified hardware path.

The following procedures are provided here:

- *Determining a Network Interface's PCI Card Slot* on page 379
- *Determining a Filesystem's PCI Card Slot* on page 379
- *Determining a Boot Device Path's PCI Card Slot* on page 380

To determine the actual physical location of a PCI card slot, based on the *cabinet-bay-chassis-slot* format that the `rad` command lists, refer to the chapter *nPartition System Overviews* on page 31 for an introduction to nPartition I/O hardware.

5420

Determining a Network Interface's PCI Card Slot

This procedure determines which PCI card slot is used by a network interface.

Step 1. At the HP-UX command line, enter the **/usr/sbin/lanscan** command to list the local nPartition's LAN devices and status.

Step 2. Enter the **rad -N *path*** command, and specify the hardware path (*path*) for the network interface whose card slot information you want.

The rad command displays the hardware slot for the network interface's card, in *cabinet-bay-chassis-slot* format.

Example 8-2 Example of Determining a Network Interface's PCI Card Slot

```
# lanscan
Hardware Station        Crd Hdw   Net-Interface  NM  MAC       HP-DLPI DLPI
Path     Address        In# State NamePPA        ID  Type      Support Mjr#
0/0/0/1/0 0x0010832754E0 0   UP    lan0 snap0     1   ETHER     Yes     119
# rad -N 0/0/0/1/0
0-1-3-0
#
```

The above output indicates that the card is installed in cabinet 0, bay 1, chassis 3, slot 0 (0-1-3-0).

Determining a Filesystem's PCI Card Slot

This procedure determines which PCI card slot is used by a filesystem.

Step 1. At the HP-UX command line, enter the **bdf -l** command to list the local filesystems for the local nPartition.

Step 2. For the filesystem of interest, enter the following command:

/usr/sbin/lvdisplay -v -k *lvolume* | grep dev

Where *lvolume* is the device path of the filesystem's logical volume, as was displayed in the bdf command output.

Step 3. Enter the **/usr/sbin/lssf *pvolume*** command, and specify the physical volume path (*pvolume*) as was reported by the lvdisplay command.

For example: lssf /dev/dsk/c0t5d0, for a filesystem whose physical volume is c0t5d0.

S419

Step 4. Enter the **rad -N *path*** command and specify the hardware path (*path*), which lssf reported as the "address" of the filesystem's physical volume.

The rad command displays the hardware slot for the filesystem's card, in *cabinet-bay-chassis-slot* format.

Example 8-3 **Example of Determining a Filesystem's PCI Card Slot**

This example determines which PCI card (0-1-3-5) supports the /stand filesystem.

```
# bdf -l
Filesystem          kbytes    used    avail %used Mounted on
/dev/vg00/lvol3     143360   42571    94743   31% /
/dev/vg00/lvol1    1025617   45445   877610    5% /stand
/dev/vg00/lvol8     512000  225212   269124   46% /var
/dev/vg00/lvol7    1015808  719619   277730   72% /usr
/dev/vg00/lvol4    1048576   77997   909975    8% /tmp
/dev/vg00/lvol6     794624  566033   214349   73% /opt
/dev/vg00/lvol5      20480    1190    18086    6% /home
# lvdisplay -vk /dev/vg00/lvol1 | grep dev
LV Name                     /dev/vg00/lvol1
VG Name                     /dev/vg00
   /dev/dsk/c0t5d0    256        256
# lssf /dev/dsk/c0t5d0
sdisk card instance 0 SCSI target 5 SCSI LUN 0 section 0 at address 0/0/6/0/0.5.0
/dev/dsk/c0t5d0
# rad -N 0/0/6/0/0.5.0
0-1-3-5
#
```

Determining a Boot Device Path's PCI Card Slot

This procedure determines which PCI card slot is used by an nPartition's boot path variable (such as PRI, HAA, or ALT).

Step 1. Issue the **/usr/sbin/parstatus -V -p# | grep Path** command, and specify the local nPartition's partition number (-p#).

This command displays the boot path variable settings for the nPartition.

To determine the local partition number, enter the parstatus -w command.

Step 2. Issue the **rad -N *path*** command and specify the hardware path (*path*) of the boot path variable of interest.

The rad command displays the hardware slot corresponding to the boot path, in *cabinet-bay-chassis-slot* format.

Example 8-4 Example of Determining a Boot Device Path's PCI Card Slot

```
# parstatus -w
The local partition number is 0.
# parstatus -V -p0 | grep Path
Primary Boot Path        : 0/0/6/0/0.6.0
Alternate Boot Path      : 0/0/6/0/0.5.0
HA Alternate Boot Path : 2/0/14/0/0.6.0
# rad -N 0/0/6/0/0.6.0
0-1-3-5
#
```

5477

Checklist for Preparing for PCI Card OLAR

This section reviews the items that you must check when adding or replacing a PCI card.

Most of the items in the following checklist are incorporated into the card addition and replacement procedures that follow.

- ☐ Review and follow all server power and safety guidelines and any related guidelines for rack operation. Also follow all site safety, maintenance, and operating procedures.
- ☐ Use proper static protection and follow all site ESD procedures.
- ☐ If *adding* a PCI card:
  - — Ensure card's required driver(s) are loaded into the currently running kernel before adding the new card.
  - — Check the target slot's frequency and power capabilities, and ensure that they match new card's requirements before adding the card.
- ☐ If *replacing* a PCI card:
  - — Check to be certain the card's driver is OLAR-capable.
  - — Be certain that the replacement card uses the same driver(s) as the original card.
  - — Be certain that the replacement card is made by the same vendor and has the same revision ID as the original card.
  - — Be certain that the replacement card operates at the same voltage and same bus frequency as the original card.
  - — Label all cables connected to the original card—or at least note their connections—before removing them.

    After replacing the card, ensure the cable are connected identically to the replacement card.
- ☐ If *replacing a networking card*, check the system (user) impact of taking the card offline before beginning to replace it.
- ☐ If *replacing a defective card*, properly label/mark the card after removing it from its slot to indicate that the card is not operational.

5416

21

Online Addition (OLA) for a PCI Card

This section describes the procedure for adding a new PCI card on an HP nPartition server while HP-UX remains online and running.

WARNING **When performing this procedure you must follow all server power and safety guidelines and any related guidelines for rack operation. Also follow all site safety, maintenance, and operating procedures.**

Failure to do so can result in personal injury or equipment damage.

PCI Card Online Addition with SAM or Partition Manager

This procedure adds a new PCI I/O card to an empty slot in an nPartition server while HP-UX remains running.

You can use either the System Administration Manager (SAM) or Partition Manager tool to perform the main steps of this procedure.

CAUTION You must follow all site static-protection requirements to avoid damaging equipment when using this procedure.

Step 1. Login to HP-UX running on the nPartition where the card that will be added is to be installed.

You must login as `root` to perform this procedure.

Step 2. Launch either SAM or Partition Manager, if it is not yet running.

You can use either application when performing this procedure.

To run SAM, enter **`/usr/sbin/sam`** from the command line. You can run SAM in either graphical (GUI) or text-only terminal mode.

To run Partition Manager either enter **`/opt/parmgr/bin/parmgr`** from the command line or click the **Partition Manager** icon in the main SAM area.

S415

Step 3. Access the list of the local nPartition's PCI card slots from SAM or Partition Manager.

To list cards in SAM, access the **Peripheral Devices > Cards** area.

To list cards in Partition Manager, select the local nPartition in the primary window, then select and open the I/O chassis where the new card will be installed.

Step 4. Identify the card slot where the new PCI card will be installed, and confirm that the slot can support the card.

You can identify the card slot using SAM's **Cards** window or Partition Manager's list of cards in its primary window. The target card slot must be available (the "Description" column for the slot is "empty slot").

You also can use the `rad -q` command to confirm that the target card slot is available (the "Occupied" column for the slot is "No").

NOTE

The **Show I/O Slot Details** option in SAM and Partition Manager displays the *default* bus speed for the selected slot, although all slots are capable of operating at either 33 MHz or 66 MHz.

When the slot "Power Available" listed is 65535 watts, the indication is that slot power details are unavailable to the utility.

See the chapter *nPartition System Overviews* on page 31 for details on the types of physical card keying the PCI card slots support.

Step 5. Confirm that the device driver(s) required by the card are installed in the HP-UX kernel currently running on the nPartition.

You can view currently loaded drivers using the SAM (`/usr/sbin/sam`) utility's **Kernel Configuration—>Drivers** area.

Step 6. [*Optional*] Confirm the physical location of both the server and the PCI card slot.

Perform the following tasks:

A. Set the card slot's attention indicator to flash in order to help you locate the slot.

5414

In SAM, select (highlight) the slot, then select the **Actions —> Light I/O Slot LED** menu item. SAM flashes the selected PCI card slot's LED.

In Partition Manager, select (highlight) the slot, then select the **I/O —> Light Chassis and Slot LEDs** menu item. Partition Manager flashes the selected PCI card slot's LED, and on HP Superdome servers also flashes the corresponding I/O chassis LED and cabinet number LCD.

From the HP-UX command line, you can issue the **`rad -f attention`** ***`slot`*** command to flash the PCI card slot's attention indicator (LED).

B. Locate the server, and view the PCI card slot attention indicators. The LED for the specified card slot should be flashing.

C. After locating the server and card slot, turn off the card slot LED.

In SAM or Partition Manager, click the **OK** button to return the attention indicators to their normal state.

From the HP-UX command line you can issue the **`rad -f off`** ***`slot`*** command to turn off the PCI card slot's attention indicator.

This step is optional, but performing it is recommended to confirm that the actual location is known and accessible.

Step 7. Begin the online PCI card addition procedure.

- To initiate online card addition in SAM, select the **Actions—>Add** menu item.

  Then select (highlight) the slot where the card will be installed, and click the **OK** button.

- To initiate online card addition in Partition Manager, select (highlight) the slot where the card will be installed, and then select the **I/O—>Add Card** menu item.

Step 8. Review the results of the critical resource analysis for the slot.

The first lines of the analysis indicate whether the card addition can or cannot proceed. For example:

```
Critical Resource Analysis for slot 0-1-3-8:
No affected resources found.
```

Step 9. Click either the **Cancel** or **OK** button.

To *cancel* the card addition procedure click the **Cancel** button.

To *continue* the card addition procedure click the **OK** button. This proceeds to power off the card's slot and flash the card's attention indicator (LED).

If you are proceeding with the card addition using Partition Manager on an HP Superdome server, Partition Manager also flashes the corresponding I/O chassis LED and cabinet number LCD.

Step 10. Review the information presented in the **Insert Card** screen.

This screen lists the actions that SAM or Partition Manager has already performed, and describes how you can cancel the card addition.

CAUTION *Complete all steps* required for installing the new PCI card before clicking the **OK** button to bring the card online.

Details for installing the new card are covered in the steps that follow.

Step 11. Locate the PCI card slot that has been prepared for the card addition procedure.

As needed, open or remove any cabinet panels or bezels in order to view the I/O chassis and card slot.

The card slot's attention indicator (LED) will be *flashing* and slot power will be *off*.

Step 12. Ensure you have direct physical access to the I/O chassis.

For example, if adding a PCI card to a Superdome I/O expansion cabinet, you must remove the I/O bay's front covers and then carefully slide the I/O chassis out from its bay/rack.

Step 13. Remove the top cover from the I/O chassis.

Loosen the cover's thumb screws, pull the cover forward, then lift and remove the cover and safely set it aside.

On HP rp7405/rp7410 and rp8400 servers, the I/O chassis cover also is the server cabinet top cover.

Step 14. Confirm the location of the card slot where the new PCI card will be installed.

At this point, all attention and power indicators (LEDs) for the card slot are visible. The light bars on the card slot's divider should indicate that the slot is powered off and its attention LED is flashing.

Each slot divider corresponds to the *PCI card slot to its immediate right* (when viewing the I/O chassis by facing the card slots with the top up).

Step 15. On HP rp7405/rp7410 and rp8400 servers, flip the card slot latch to its open position.

When open, the latch is parallel to the back edge of the chassis.

Step 16. Place the new card in the slot.

Slide the card in the slot, and ensure it is properly aligned. Press firmly on the card until it is fully seated in the card slot.

Step 17. On HP rp7405/rp7410 and rp8400 servers, flip the card slot latch to its closed position.

When closed, the latch is parallel to the card slot divider.

If the latch will not close, the card might not be completely seated in its slot. In this situation, you can either press firmly on the card until it is seated, or lift the slot divider to release the card and then realign and reseat the card.

Step 18. Connect all cables to the new card to establish the desired configuration.

Step 19. Replace the top of the I/O chassis, and restore all front covers and bezels to their original locations.

Replace the I/O chassis cover and firmly push it back into place before tightening all thumb screws.

Also, as needed, carefully slide all racked equipment back into place before replacing any additional covers and bezels. Close any cabinet or rack doors.

Step 20. In the SAM or Partition Manager **Insert Card** window, click the **OK** button.

Clicking **OK** indicates that the new card has been installed.

At this point, the card slot is powered on, the slot attention indicator is turned off, and the driver(s) for the card are started to bring the card online.

If the new card is not detected in the slot, SAM or Partition Manager indicates this and presents a window indicating the problem. This gives you an opportunity to check the new card's installation and then click **Yes** to re-try the card online addition, or click **No** to cancel the operation.

Online Replacement (OLR) for a PCI Card

This section describes the procedure for replacing a PCI card on an HP nPartition server while HP-UX remains online and running.

WARNING **When performing this procedure you must follow all server power and safety guidelines and any related guidelines for rack operation. Also follow all site safety, maintenance, and operating procedures.**

Failure to do so can result in personal injury or equipment damage.

PCI Card Online Replacement with SAM or Partition Manager

This procedure replaces a PCI I/O card in an nPartition server while HP-UX remains running.

You can use either the System Administration Manager (SAM) or Partition Manager tool to perform the main steps of this procedure.

CAUTION You must follow all site static-protection requirements to avoid damaging equipment when using this procedure.

Step 1. Login to HP-UX running on the nPartition where the card that will be replaced is currently installed.

You must login as `root` to perform this procedure.

Step 2. Launch either SAM or Partition Manager, if it is not yet running.

You can use either application when performing this procedure.

To run SAM, enter **`/usr/sbin/sam`** from the command line. You can run SAM in either graphical (GUI) or text-only terminal mode.

S409

To run Partition Manager either enter `/opt/parmgr/bin/parmgr` from the command line or click the **Partition Manager** icon in the main SAM area.

Step 3. Access the list of the local nPartition's PCI cards from SAM or Partition Manager.

To list cards in SAM, access the **Peripheral Devices > Cards** area.

To list cards in Partition Manager, select the local nPartition in the primary window, then select and open the I/O chassis where the card that will be replaced is currently installed.

Step 4. Identify the card's slot location and confirm that the card can be replaced online.

Perform the following tasks:

A. View the list of currently available PCI card slots in the local nPartition.

This card list is shown in SAM's **Cards** window or in Partition Manager's primary window.

B. Identify the slot where the card that will be replaced is currently installed.

The "Description" column indicates the type of card in the slot.

C. Confirm that the driver for the PCI card slot supports OLAR procedures.

The "State" column indicates "not OLAR-able" if the card *cannot* be replaced online, otherwise online replacement of the card is supported.

Step 5. [*Optional*] Confirm the physical location of both the server and the PCI card slot.

Perform the following tasks:

A. Set the card slot's attention indicator to flash in order to help you locate the slot.

In SAM, select (highlight) the slot, then select the **Actions —> Light I/O Slot LED** menu item. SAM flashes the selected PCI card slot's LED.

In Partition Manager, select (highlight) the slot, then select the **I/O —> Light Chassis and Slot LEDs** menu item. Partition Manager flashes the selected PCI card slot's LED, and on HP Superdome servers also flashes the corresponding I/O chassis LED and cabinet number LCD.

From the HP-UX command line, you can issue the `rad -f attention slot` command to flash the PCI card slot's attention indicator (LED).

B. Locate the server, and view the PCI card slot attention indicators. The LED for the specified card slot should be flashing.

C. After locating the server and card slot, turn off the card slot LED.

In SAM or Partition Manager, click the **OK** button to return the attention indicators to their normal state.

From the HP-UX command line you can issue the `rad -f off slot` command to turn off the PCI card slot's attention indicator.

This step is optional, but performing it is recommended to confirm that the actual location is known and accessible before the card's services are suspended.

Step 6. Select the PCI card to be replaced from the card list displayed by SAM or Partition Manager.

Highlight the card in the list. If you are replacing a multi-function card, you only need to highlight any one of the hardware paths in the slot.

For a multi-function (multi-port) card, SAM and Partition Manager list one entry per port, with each port having the same slot number in the "Slot" column and a unique path in the "Hardware Path" column.

Step 7. Begin the online replacement procedure for the selected card.

To initiate online card replacement in SAM, select the **Actions—>Replace** menu item.

To initiate online card replacement in Partition Manager, select the **I/O—>Replace Card** menu item.

Both of these menu items initiate the same processes, beginning with an analysis of any resources provided by the selected card.

Step 8. Review all results from the critical resource analysis of the card.

5407
38

The first lines of the analysis indicate whether the card replacement can or cannot proceed. For example:

```
Critical Resource Analysis for slot 0-1-3-8:
No affected resources are in use.
```

If the card resource analysis determines that the card cannot be taken offline, this result is indicated with a "critical" message such as the following output.

```
CRITICAL: Affected resources are essential for system
operation.
The operation cannot proceed.
```

For a multi-function card, SAM and Partition Manager list the analysis results for all ports on the card.

CAUTION

Review *all parts* of the critical resource analysis report to determine whether to continue or cancel an online card replacement procedure.

Even when the analysis indicates that "no affected resources are in use", continuing the card replacement procedure will take the card offline and will halt any services the card provides.

For example, replacing a networking card causes any network connections the card provides to be suspended or terminated.

Step 9. Click either the **Cancel** or **OK** button.

To *cancel* the card replacement procedure click the **Cancel** button. This cancels the procedure and returns to the list of PCI cards. After you click **Cancel** *you must not perform the remaining steps* in this procedure.

To *continue* the card replacement procedure click the **OK** button. This proceeds to suspend the card's driver(s), power off the card's slot, and flash the card's attention indicator (LED).

Step 10. Review the information presented in the **Replace Cards** screen.

This screen lists the actions that SAM or Partition Manager has already performed to take the selected card offline.

CAUTION *Complete all steps* required for replacing the selected PCI card before clicking the **OK** button to bring the card back online. Details for removing and replacing the card are covered in the steps that follow.

NOTE Clicking the **Cancel** button on the **Replace Cards** screen causes the card to *remain offline*: the card slot remains powered off and the card driver(s) remain suspended. The card slot attention indicator is turned off.

Because the card's slot power remains off, you still can replace the card.

To bring a card back online, select the card and then choose the **Actions—>Bring On-line** menu item in SAM or the **I/O—>Bring Card On-line** menu item in Partition Manager.

Step 11. Locate the PCI card slot that has been taken offline for the card removal procedure.

As needed, open or remove any cabinet panels or bezels in order to view the I/O chassis and card slot that contains the PCI card to be replaced.

The card slot's attention indicator (LED) will be *flashing* and slot power will be *off*.

Step 12. Ensure you have direct physical access to the I/O chassis.

For example, if replacing a PCI card from a Superdome I/O expansion cabinet, you must remove the I/O bay's front covers and then carefully slide the I/O chassis out from its bay/rack.

Step 13. Remove the top cover from the I/O chassis.

Loosen the cover's thumb screws, pull the cover forward, then lift and remove the cover and safely set it aside.

On HP rp7405/rp7410 and rp8400 servers, the I/O chassis cover also is the server cabinet top cover.

Step 14. Locate the PCI card that is to be replaced, note all cable connections to the card, and if needed label any unmarked cables. Save all notations for future reference.

S405

At this point, all attention and power indicators (LEDs) for the card slot are visible. The light bars on the replacement card's slot divider should indicate that the slot is powered off and its attention LED is flashing.

Each slot divider corresponds to the *PCI card slot to its immediate right* (when viewing the I/O chassis by facing the card slots with the top up).

Step 15. Disconnect all cables from the PCI card to be replaced.

Carefully set the cable ends aside where they will not obstruct work or be damaged.

Step 16. On HP rp7405/rp7410 and rp8400 servers, flip the card slot latch to its open position.

When open, the latch is parallel to the back edge of the chassis.

Step 17. Lift the card slot divider to release the PCI card from its slot.

Pull firmly on the slot divider's "handle" until the card becomes unseated. The correct slot divider is indicated by its LED states.

Step 18. Remove the card from its slot and set the card aside.

You may need to label the removed card to indicate it is defective.

Step 19. Place the replacement card in the slot.

Slide the card in the slot, and ensure it is properly aligned. Press firmly on the card until it is fully seated in the card slot.

Step 20. On HP rp7405/rp7410 and rp8400 servers, flip the card slot latch to its closed position.

When closed, the latch is parallel to the card slot divider.

If the latch will not close, the card might not be completely seated in its slot. In this situation, you can either press firmly on the card until it is seated, or lift the slot divider to release the card and then realign and reseat the card.

Step 21. Reconnect all cables to the new card to match their prior attachments to the original card.

Step 22. Replace the top of the I/O chassis, and restore all front covers and bezels to their original locations.

Replace the I/O chassis cover and firmly push it back into place before tightening all thumb screws.

Also, as needed, carefully slide all racked equipment back into place before replacing any additional covers and bezels. Close any cabinet or rack doors.

Step 23. In the SAM or Partition Manager **Replace Card** window, click the **OK** button.

Clicking **OK** indicates that the card has been removed and replaced with a new card.

At this point, the card slot is powered back on, the slot attention indicator is turned off, and the driver(s) for the card are resumed to bring the card online.

However, if SAM or Partition Manager cannot bring the replacement card online then you may need to perform additional steps, as directed the SAM or Partition Manager user interface.

9 Processor Instant Capacity on Demand (iCOD)

This chapter covers using Hewlett-Packard's processor iCOD (Instant Capacity on Demand) product on nPartitions.

iCOD is an *optional* software product that enables you to instantly increase or adjust processing power within nPartitions. As you need more or fewer processors, you use iCOD tools to adjust the number of activated processors in the nPartition.

Two varieties of iCOD software and contracts are available from HP: iCOD Purchase and iCOD Utility (pay per use). Both are described in this chapter.

NOTE Using both Processor Sets (Psets) and iCOD simultaneously is supported for iCOD Purchase Version 5.0 and higher only.

NOTE For HP Superdome nPartitions running the HP virtual partitions software, only iCOD Purchase Version 5.0 and higher is supported.

5401

Introduction to Processor iCOD on nPartitions

HP's iCOD product is available for both nPartition servers and non-partitionable HP servers. This document covers iCOD issues that are unique to nPartition systems.

See the *Instant Capacity on Demand (iCOD) and Pay Per Use (PPU) User's Guide for Version B.04.x* and the *Instant Capacity on Demand (iCOD) User's Guide for Version B.05.00* for complete information about iCOD on all supported platforms.

iCOD is an *optional* product that includes an iCOD software bundle and a corresponding system contract with Hewlett-Packard, which determine the type of billing for processors you activate and use.

Billing for iCOD-activated processors is calculated on a complex-wide basis: the total number of activated iCOD processors in all nPartitions.

HP nPartition systems support two varieties of iCOD:

- **iCOD Purchase**

  iCOD Purchase enables you to instantly activate and purchase *additional* processors as your needs increase.

- **iCOD Utility (PPU: Pay Per Use)**

  iCOD Utility supports instantly increasing and decreasing the number of activated processors, for billing on a *pay per use* basis.

All nPartitions in a server complex either must run the same iCOD variety (purchase or utility) or not run iCOD. If you configure iCOD Utility for one nPartition then you also must configure all other nPartitions with iCOD Utility. HP recommends (but does not require) that you configure iCOD Purchase for all nPartitions if you configure any nPartition with iCOD Purchase.

You cannot configure nPartitions with both iCOD Utility and iCOD Purchase in the same server complex.

5400

iCOD Features for nPartitions

HP's iCOD Purchase and iCOD Utility products have some different features and behaviors on nPartition servers than iCOD on other non-partitionable systems.

The following list covers some of these unique features.

- iCOD on each nPartition is managed locally and independently.

  iCOD commands affect and list iCOD settings for the *local* nPartition (the nPartition where the commands are run).

  While there is one iCOD license for the entire server complex, iCOD processors are activated and deactivated independently for each nPartition. Each nPartition has its own settings for iCOD contact, notification, and processor configuration purposes.

- Passwords are not required for activating and deactivating iCOD processor on nPartitions.

  On nPartition servers under either iCOD contract (iCOD Purchase or iCOD Utility) you can perform all tasks that change the iCOD processor configuration for an nPartition.

  On non-partitionable systems an HP service password is required for some iCOD processor deactivation tasks.

- Both varieties of iCOD support "load balancing" processors across nPartitions in the same server complex.

  When using either iCOD Purchase or iCOD Utility, you can instantly adjust each nPartition's number of activated processors as system loads demand and maintain the same total number of activated processors in the complex.

  For example, you can deactivate processors in one underused nPartition and activate the same number of processors in another, more heavily used nPartition to load balance using the same number of processors.

  This load balancing does not change any nPartition cell assignments. Each nPartition keeps the hardware assigned to it while iCOD software in each nPartition either activates or deactivates processors.

5399

iCOD Issues for Managing nPartitions

iCOD introduces several new issues for managing nPartitions. The following list describes some of these new management issues for nPartition systems that have iCOD configured:

- At least one iCOD processor must be activated for each active cell in an nPartition.

  For example, a three-cell nPartition with iCOD must have at least three activated iCOD processors, and the iCOD software ensures that each cell has a processor activated.

- The maximum number of activated processors in an nPartition is the iCOD "requested active processors" setting.

  However, if the number of active cells is *greater than* the number of "requested active processors" then the iCOD software activates more processors than were requested: one processor is activated for each active cell in the nPartition.

- Only processors on active cells can be activated by iCOD.

  Inactive cells in an nPartition cannot have processors activated by iCOD in the nPartition. To activate processors on inactive cells, you first must make the cells active.

- Activating and deactivating processors can potentially affect software packages that rely on certain processor IDs to be present, such as certain processor set (Pset) configurations. Refer to the chapter *Processor Sets (Psets) on nPartitions* on page 419 for details.

  Likewise, changing the number of activated processors may have implications for managing software that is licensed on a per-processor basis.

- Adding or removing cells in an nPartition with iCOD does not necessarily increase or decrease the number of activated processors in the nPartition.

  The iCOD software activates the requested number of processors for an nPartition as long as the nPartition has enough configured processors to satisfy the request.

  Adding a cell to an nPartition increases the total processors and the number of configured processors in the nPartition. However, if the requested number of processors remains the same for the nPartition then the same number of activated iCOD processors are available after performing a reboot for reconfig to make the newly added cell active.

For example, in a two-cell nPartition that has six of its eight processors activated with iCOD, adding another four-processor cell brings the total processors to 12. However, the iCOD software keeps the number of activated processors at six (no change). (Other of the new cell's resources—such as memory and I/O—are made available for use in the nPartition.)

Likewise, removing a cell from an nPartition reduces the total processors and the number of configured processors in the nPartition. If enough processors remain available then the requested number of iCOD processors are activated.

When not enough processors are configured, the iCOD software activates as many processors as possible and the number of activated processors is less than the number of "requested active processors".

The sections that follow give more details for managing iCOD on nPartitions.

Tools for Managing iCOD Processors

The HP Instant Capacity on Demand (iCOD) product includes the following commands for managing iCOD settings and processor configurations. This same set of commands is used for both the iCOD Purchase and iCOD Utility products.

For details on these commands, see the *icod_modify* (1M), *icod_notify* (1M), and *icod_stat* (1M) manpages.

- `/usr/sbin/icod_modify`

  The `icod_modify` command allows you to activate and deactivate iCOD processors. This command also lets you change system contact information and apply a software license to use iCOD.

  The `-a` option activates processors and `-d` deactivates processors.

- `/usr/sbin/icod_notify`

  The `icod_notify` command allows you to request that an iCOD asset report be delivered by e-mail, and allows you to turn on or off e-mail notification of iCOD configuration changes.

  The `-n` option turns on or off automatic change notification e-mail.

- `/usr/sbin/icod_stat`

  The `icod_stat` command displays iCOD status and configuration information as well as iCOD processor usage details.

  The `-p` option gives complex-wide iCOD Purchase details on nPartition systems. The `-u` option displays the iCOD change record, listing the changes from oldest to newest.

When using the iCOD commands to activate and deactivate processors or update contact and notification details, you affect the iCOD configuration and settings for the *local nPartition* only. While some iCOD settings are stored in complex profile data, many iCOD settings are stored on disk in the iCOD configuration file (/etc/.iCOD_data). As a result, you may need to check and adjust iCOD configuration settings when booting from different disks.

When you license iCOD (by using the `icod_modify -l...` command) you can do so from *any nPartition* in the server complex. This licenses iCOD for all nPartitions in the server, and only one license is needed for the entire complex.

5395

iCOD Requirements for nPartition Servers

HP's iCOD software has the following requirements and restrictions for using and managing iCOD processors in an nPartition server complex.

- Each nPartition server complex can *optionally* be under either an iCOD Purchase contract or a pay per use (iCOD Utility) contract.

  In a server complex that is under one of these contracts, the appropriate software **must** be installed in the complex's nPartitions to support the contract.

  HP *does not* support mixing iCOD Purchase and iCOD Utility nPartitions in the same server complex.

- nPartition servers that are under an iCOD Utility contract (a pay per use "PPU" contract) **must** have iCOD Utility software installed and running on *every* HP-UX instance in the complex.

NOTE

Where multiple devices are configured for an nPartition (for example, the PRI, HAA, and ALT boot paths), each device must have iCOD Utility software installed. This applies to nPartition servers under a PPU (iCOD Utility) contract.

- Each nPartition that is under an iCOD Purchase contract **must** have iCOD Purchase software installed to enable additional processors to be activated (or to deactivate processors).

  In an iCOD Purchase complex, you *do not* have to install iCOD Purchase software on the nPartitions that are *not* under an iCOD Purchase contract. However, in this situation HP recommends that all nPartitions have iCOD Purchase software installed to allow administrators to perform "load balancing" across nPartitions.

NOTE

All potential boot disks for nPartitions with iCOD processors must have the iCOD Purchase software installed, including any alternate boot devices. This applies to nPartition servers under an iCOD Purchase contract.

5394
20

- For the iCOD software to activate processors, the processors **must** be *configured* processors on *active* cells that are *assigned* to the local nPartition

  Processors that are deconfigured cannot be activated by iCOD; they first must be configured (for example, by using the BCH Configuration menu's `CPUCONFIG` command).

  Cells that are inactive cannot have processors activated by iCOD. Each cell first must boot and complete "partition rendezvous" before it can contribute resources to the nPartition to which it is assigned.

  Likewise, cells that are unassigned cannot have processors activated by iCOD. Each cell must be assigned to an nPartition and must be an active member of its nPartition before its resources can be used.

5393

Installing and Configuring iCOD on nPartitions

NOTE This section describes iCOD software install and configuration for an nPartition server complex.

You also must establish a contract with HP for either iCOD Purchase or iCOD Utility (pay per use) to properly use this software product.

Software bundles for iCOD Purchase and iCOD Utility are available on the Support Plus media and at the `http://software.hp.com` Web site.

For complete details on installing and using iCOD software, refer to the *Instant Capacity on Demand (iCOD) and Pay Per Use (PPU) User's Guide for Version B.04.x* and the *Instant Capacity on Demand (iCOD) User's Guide for Version B.05.00*.

The following procedure gives an overview of initially installing and configuring iCOD Purchase or iCOD Utility on an nPartition server complex.

iCOD Installation and Configuration

Step 1. Install the appropriate iCOD software bundle on all required nPartitions in the server complex.

On nPartition server complexes that have iCOD Purchase contracts, you must install the iCOD Purchase software on those nPartitions in the complex that have iCOD processors. (For greater flexibility in load balancing iCOD processors HP recommends installing iCOD Purchase software on all nPartitions.)

On nPartition servers that have iCOD Utility (pay per use) contracts, you must install the iCOD Utility software on *every* nPartition in the complex.

If you expect to boot an nPartition from different devices—even on rare occasions—you must install the appropriate iCOD software bundle on all potential boot devices (such as the devices at the PRI, HAA, and ALT boot paths).

5392

Step 2. [*An HP service representative must perform this step.*]

Validate the server complex as an iCOD server.

Step 3. Configure `sendmail` so that it can send e-mail to an HP mail server that is outside of your company's firewall.

HP iCOD software sends encrypted e-mail from the local nPartition running iCOD to HP for billing purposes and to request licensing information. Details on `sendmail` configuration are in the user's guide for iCOD.

You must configure `sendmail` on all nPartitions that have iCOD software installed. On nPartitions with multiple boot devices, configure `sendmail` for each boot device.

Step 4. Configure the iCOD contact information for each nPartition that has iCOD software installed, using the `icod_modify -c...` command.

This specifies the person who will receive iCOD licensing e-mail from HP and iCOD configuration change notices. For example:

```
# icod_modify -c "Joe Doe":joe@company.com:555-5555
```

On nPartitions with multiple boot devices, configure the the iCOD contact information for each boot device, in case alternate devices (such as HAA or ALT) are booted.

Step 5. [*This step needs to be performed only once for the entire server complex.*]

Request a license by issuing the `icod_notify` command (with no options) in any nPartition that has iCOD, `sendmail`, and the contact information configured.

The `icod_notify` command sends an iCOD asset report to HP and to the iCOD contact and `root` for the nPartition. After HP receives the asset report a confirmation e-mail, which contains the iCOD license key, is sent to the iCOD contact.

Apply the license for iCOD by issuing the `icod_modify -l...` command. For example:

```
# icod_modify -l AABBCCDD
```

where *AABBCCDD* is the iCOD license key given in the confirmation e-mail. You only need to apply the iCOD license once for the entire server complex.

5391

Step 6. Use iCOD features: list iCOD statistics with `icod_stat` and, when required, activate or deactivate processors.

To list iCOD configuration details for the local nPartition, use the `icod_stat` command (with no options).

For an nPartition complex that has iCOD Purchase configured for multiple nPartitions, you also can use the `icod_stat -p` command to display iCOD processor usage statistics for all nPartitions in the server complex. (The `-p` option does not give more information for iCOD Utility configurations or for non-nPartition configurations.)

See *Procedures for Changing Processor iCOD Configurations on nPartitions* on page 409 for details on managing an nPartition's iCOD processors.

Ne

5390

Procedures for Changing Processor iCOD Configurations on nPartitions

This section covers the following procedures for changing the iCOD configuration on nPartitions. These procedures apply for both iCOD Purchase and iCOD Utility software and contracts.

- *Activating and Deactivating Processors with iCOD* on page 410

  This procedure (using the icod_modify -a... or icod_modify -d... command) activates or deactivates processors in an nPartition with iCOD.

- *Setting the Total Number of Requested Active Processors* on page 411

  This procedure (using the icod_modify -s... command) sets the total number of requested active processors for an nPartition with iCOD software installed and configured.

- *Load Balancing Processors across nPartitions with iCOD* on page 412

  This procedure (using both the icod_modify -d... and icod_modify -a... commands) adjusts the balance of activated processors across two nPartitions in the same server complex: deactivate processors in one nPartition and activate the same number of processors in another nPartition.

- *iCOD Contract Changes for an nPartition Server Complex* on page 413

  This procedure describes how to change your existing iCOD contract to either iCOD Purchase or iCOD Utility by contacting HP sales or support representatives.

- *Removing iCOD Software and Functionality from nPartitions* on page 414

  This procedure describes how to remove iCOD software and functionality from an nPartition server complex after completing your iCOD purchasing and contract obligations.

5389

NOTE The following nPartition changes also can cause iCOD software to activate a different number or set of the nPartition's processors: adding and removing cells from an nPartition, making cells active or inactive, or configuring or deconfiguring processors from cells in the nPartition.

Activating and Deactivating Processors with iCOD

This procedure (using the `icod_modify -a...` or `icod_modify -d...` command) activates or deactivates processors in an nPartition with iCOD.

NOTE Activating or deactivating processors can affect your billing for iCOD services.

On systems with HP processor set (Pset) software installed: *newly activated* processors are assigned to the default Pset, and deactivated processors are removed from the Pset to which they were assigned.

HP's iCOD software selects processors for activation or deactivation by following the appropriate processor installation order for the machine type. The iCOD utilities select processors based on their *physical location* in the server (not their HP-UX CPU IDs).

For example, on HP Superdome servers the processor install order for each cell is: first processor slot 0, then slots 3, 1, and 2.

As a result, all active cells in a Superdome nPartition always have processor 0 activated because a minimum of one processor must be activated per cell. Then, as needed to meet the iCOD "requested active processors" number for the nPartition, each cell's "processor 3" slot is activated, then each cell's "processor 1" slot, and finally the "processor 2" slots.

Step 1. Login to the nPartition in which you will be activating or deactivating processors.

You can activate or deactivate processors in only the *local* nPartition (the nPartition in which you issue the `icod_modify` command).

5388
2l

Step 2. Issue the `icod_modify` command with either the `-a #` option (to activate # processors) or `-d #` option (to deactivate # processors).

You must include the following details after the `-a` or `-d` option. This information is recorded in the nPartition's iCOD change log.

`[`*`description`*`]:`*`user_name`*`:`*`mgr_name`*`:`*`mgr_email`*`:`*`mgr_phone`*

These details provide an optional description of the change, the name of the user/person making the change, and the authorizing manager, manager's e-mail address, and manager's phone number.

For example, to activate two processors (`-a 2`):

```
# icod_modify -a 2 "two CPUs added":Ann:Joe:jdoe@comp.com:555-5555
```

In the next example, one processor is deactivated (`-d 1`):

```
# icod_modify -d 1 "one less CPU":Ann:Joe:jdoe@comp.com:555-5555
```

See also the *icod_modify* (1M) manpage for details.

Step 3. As desired, issue the `icod_stat` command to list the new processor configuration details for the local nPartition.

Setting the Total Number of Requested Active Processors

This procedure (using the **`icod_modify -s...`** command) sets the total number of requested active processors for an nPartition with iCOD software installed and configured.

Performing this procedure can increase or decrease the number of activated processors in an nPartition.

NOTE Activating or deactivating processors can affect your billing for iCOD services.

On systems with HP processor set (Pset) software installed: *newly activated* processors are assigned to the default Pset, and deactivated processors are removed from the Pset to which they were assigned.

Step 1. Login to the nPartition in which you will be activating or deactivating processors.

S387

You can activate or deactivate processors in only the *local* nPartition (the nPartition in which you issue the `icod_modify` command).

Step 2. Issue the `icod_modify -s...` command and specify the number of processors to be activated.

You must include the following details after the `-s` option. This information is recorded in the nPartition's iCOD change log.

[*description*]:*user_name*:*mgr_name*:*mgr_email*:*mgr_phone*

For example, the following command sets the number of "requested active processors" to 10, which may increase or decrease the number of activated processors in the nPartition (depending on the number of processors available before the command is issued).

```
# icod_modify -s 10 "activate 10 CPUs total":Ann:Joe:jdoe@comp.com:555-5555
```

See also the *icod_modify* (1M) manpage for details.

Step 3. As desired, issue the `icod_stat` command to list the new processor configuration details for the local nPartition.

Load Balancing Processors across nPartitions with iCOD

This procedure (using both the **`icod_modify -d...`** and **`icod_modify -a...`** commands) adjusts the balance of activated processors across two nPartitions in the same server complex: deactivate processors in one nPartition and activate the same number of processors in another nPartition.

NOTE

After "load balancing" processors across nPartitions, each nPartition still has the same cells and processors assigned to it.

However, this procedure reduces the number of activated processors in the first nPartition and increases (by the same amount) the number of activated processors in the second nPartition.

This procedure does not affect your billing for iCOD services *if*: the total number of activated processors in the complex does not change *and* the operations are not performed by HP service representatives.

Both nPartitions must have iCOD software installed and configured.

Also, both nPartitions must have enough activated or deactivated processors to accommodate the reduction or increase in processors.

Step 1. Login to the first nPartition and deactivate the number of processors you plan to activate in the second nPartition.

See the procedure *Activating and Deactivating Processors with iCOD* on page 410, and use the `icod_modify -d...` command to deactivate the processors.

If HP processor set (Pset) software is installed, deactivating processors removes the corresponding CPU IDs from the Pset to which they were assigned.

Step 2. Login to the second nPartition and activate the same number of processors you deactivated in the previous step.

See the procedure *Activating and Deactivating Processors with iCOD* on page 410 and use the `icod_modify -a...` command to activate the processors.

If HP processor set (Pset) software is installed, the newly-activated processors are assigned to the local nPartition's default Pset.

iCOD Contract Changes for an nPartition Server Complex

This procedure describes how to change your existing iCOD contract to either iCOD Purchase or iCOD Utility by contacting HP sales or support representatives.

Changing the type of iCOD contract for a server complex will affect your billing for iCOD services.

Step 1. Contact your HP sales or support representatives and request an iCOD contract and software change.

Changing the type of iCOD contract and software will require that an HP service representative alter the iCOD software configuration for all nPartitions affected by the change.

For nPartitions that have multiple boot devices (such as PRI, HAA, and ALT), HP iCOD software bundles on every boot device must be updated.

5385

Step 2. Consider any software licensing issues or nPartition system configuration issues that you must address when changing from iCOD Purchase to iCOD Utility (pay per use) or vice versa.

For example, some nPartitions may have different sets of processors activated as a result of the change. Or, in the case of a pay per use (iCOD Utility) contract, the set of activated processors in each nPartition may change on an ongoing basis.

Such changes could potentially affect HP processor set (Pset) configurations, or the configuration of HP Process Resource Manager (PRM) or HP Workload Manager (WLM) software.

Removing iCOD Software and Functionality from nPartitions

This procedure describes how to remove iCOD software and functionality from an nPartition server complex after completing your iCOD purchasing and contract obligations.

For more details, see the *Instant Capacity on Demand (iCOD) and Pay Per Use (PPU) User's Guide for Version B.04.x* and the *Instant Capacity on Demand (iCOD) User's Guide for Version B.05.00*.

Step 1. Confirm that all processors in all nPartitions in the server complex are activated and purchased.

All processors in the complex are activated when: for every nPartition the "requested active processors" equals the "total processors". You can check this by issuing the `icod_stat` command in each nPartition.

If you have a server complex that is under an iCOD Purchase contract, you also must have paid the enablement fee for all processors. Confirm this with your HP sales or service representative.

If your server complex is under an iCOD Utility (pay per use) contract, you must check with your HP sales or service representative to determine if you have met all contract requirements.

Step 2. After confirming with HP that you have completed all requirements, use the `swremove` command to uninstall the iCOD Purchase or iCOD Utility bundle.

5384

You must remove the bundle from every nPartition that no longer is under contract. In the case of iCOD Utility contracts this involves removing the bundles from all nPartitions.

On nPartitions where iCOD software is installed on multiple boot devices (such as PRI, HAA, and ALT) you should remove the bundle from all devices.

See the iCOD documentation and the *swlist* (1M) and *swremove* (1M) manpages for details.

5383

Managing iCOD Utility (Pay Per Use) on nPartitions

This section describes several methods of managing processor resources for a server complex that is under a pay per use (iCOD Utility) contract.

If your server complex is under an iCOD Utility contract then you are billed for *all activated* processors in the whole nPartition server complex.

The pay per use iCOD Utility contract enables you to manage processor resources in the complex in such a way that you only pay for the amount of processor resources that you actually require.

When you have processors in an nPartition complex that you do not need, you can exclude those processors from billing by *deactivating* processors, by making processors *inactive*, or by *deconfiguring* processors.

These three methods of excluding processors from pay per use billing are discussed here. See the *Deactivated Processors*, *Inactive Processors*, and *Deconfigured Processors* sections that follow.

Tips for Pay Per Use Processor Management

- The recommended method for activating and deactivating processors on nPartitions is to use the `icod_modify` command. This command instantly increases or decreases the number of available processor resources in the nPartition without requiring a reboot.

  For example, if an nPartition is underused—as when most of the nPartition's processors are constantly idle—you could deactivate unneeded processors by using the `icod_modify -d...` command.

- When an entire nPartition in a complex is unused you can exclude that nPartition's processors from billing by making the nPartition inactive.

  For example, if an nPartition is not running HP-UX but is "just sitting at the BCH interface" you could reset the nPartition to the ready for reconfig state by using the BCH `RECONFIGRESET` command to make the nPartition inactive. (When an nPartition is running HP-UX, using the `shutdown -R -H` command makes the nPartition inactive.)

When an nPartition is inactive, all its cells and processors are inactive and cannot be used until the nPartition is booted (using the GSP or MP Command menu's BO command).

- Individual cells that are *inactive* are not billed for iCOD Utility purposes, because all processors on inactive cells also are inactive.

  This includes unassigned cells, as well as cells that have not participated in "partition rendezvous" for their assigned nPartition (for example: newly-added cells or cells that had a "n" use-on-next-boot value when the nPartition last booted).

Deactivated Processors

A **deactivated processor** is one that has been "turned off" by the nPartition's iCOD software, perhaps as a result of the `icod_modify -d...` command. Deactivated processors can be activated instantly by using the `icod_modify -a...` command.

The iCOD software selects which processors are activated and deactivated and chooses processors based on their physical locations.

For details, see the procedures in *Activating and Deactivating Processors with iCOD* on page 410.

Inactive Processors

An **inactive processor** is a processor that is in an inactive cell and thus is at a boot is blocked (BIB) state.

The following examples describe situations where both cells and processors are inactive (and thus are not subject to iCOD Utility billing):

- All processors on a cell that is not assigned to an nPartition are inactive.
- All processors on a cell that did not participate in "partition rendezvous" for its nPartition are inactive.

  You can make a cell inactive either by unassigning it from an nPartition, or by setting the cell's use-on-next-boot value to "n" (meaning: do not use the cell) and rebooting the cell's nPartition.
- All processors on cells that are assigned to an inactive nPartition are inactive.

  You can make all processors in an nPartition inactive by resetting the nPartition to the ready for reconfig state. In an inactive nPartition, all cells are inactive and thus all processors on cells in the nPartition are inactive.

3381

> To put an nPartition in the inactive, ready for reconfig state: if HP-UX is running use the `shutdown -R -H` command, or if at the Boot Console Handler (BCH) interface use the `RECONFIGRESET` command.

None of an inactive cell's resources (processors, memory, or any I/O connected to the cell) are available for use in an nPartition. For the cell's processors and other hardware resources to be used, the cell must be *assigned* and *active* in an nPartition.

Deconfigured Processors

A **deconfigured processor** is a processor that has been made unavailable for use by its nPartition through settings enabled by Boot Console Handler (BCH) menu commands.

You can deconfigure processors using the BCH Configuration menu's `CPUCONFIG` command. Also use this command to configure processors that have been deconfigured.

Using BCH commands to configure and deconfigure processors requires rebooting the nPartition in which the processors reside. For this reason deconfiguring processors is *not the recommended method* of making processors inactive for iCOD purposes.

Instead, the recommended method is to deactivate processors using the `icod_modify -d...` HP-UX command, which can instantly make processors deactivated and activated without rebooting.

S380

10 Processor Sets (Psets) on nPartitions

This chapter describes how to use and manage processor sets (Psets) on nPartition systems.

Using Psets, you can create multiple independent processor groups in an nPartition. Each Pset has its own processors, schedules, and attributes. Because Psets are dynamic, you can create, modify, and destroy Psets instantly as your system needs demand.

HP's processor set software is an *optional* package that is free for all HP-UX 11i systems and is available at the `http://software.hp.com` Web site.

The same Pset features are available on all HP-UX 11i systems, including both non-partitionable systems and nPartitions servers.

On nPartition servers, however, you should be aware of the nPartition system configuration issues that can affect your use of processor sets. This chapter covers special configuration issues for Psets in nPartition environments.

NOTE Using both Processor Sets (Psets) and iCOD simultaneously is supported for iCOD Purchase Version 5.0 and higher only.

S379

Introduction to Psets

HP's processor set (Pset) product is an optional software package that runs on any HP-UX 11i system, including all nPartition servers. The Pset software package is free and is available from the **`http://software.hp.com`** Web site.

Each processor set (Pset) is a group of active processors that functions as an independent *scheduling allocation domain*. When the Pset software is installed, you can establish multiple Psets in a single HP-UX system.

By dividing the active processors in an nPartition into multiple Psets, you can provide processor resource isolation for applications that run in each Pset. Each application only has access to the processors assigned to the Pset in which it runs.

You can dynamically create and reconfigure Psets using the `psrset` command or HP's Process Resource Manager (PRM). You also can launch each thread or process to run in a specific Pset and can manually migrate threads and processes to different Psets while they run.

Thread and Process Pset Bindings

In systems where Pset software is installed, every thread and process is bound to only one Pset at a time.

Applications are not migrated to different Psets unless you have configured PRM to do so, or if you manually bind a process to a different Pset using the `psrset` command.

HP-UX load balancing occurs within each Pset. Because load balancing does not occur across Psets, processors in one Pset can potentially be oversubscribed while processors in another Pset are nearly idle. This is an aspect of the processor resource isolation that Psets provide.

Both real-time and time-share schedulers are supported for processor sets and each Pset has its own schedulers. So, for example, real-time processes in one Pset only contend for processors in the Pset in which they are running.

Use of the HP-UX gang scheduler is supported only in the default Pset (processor set ID 0), as of the current Pset software release. See the *gang_sched* (7) manpage or the *mpsched* (1) manpage for details on using gang scheduling.

5378
20

HP-UX Processor Numbering and Availability on nPartitions

The HP-UX operating system number processors from 0 to n-1, where n is the number of configured processors on active cells in an nPartition.

Each physical processor is not necessarily given the same logical HP-UX processor ID each time the nPartition is booted. HP-UX processor IDs are assigned on a first-come first-numbered basis. As a result, even if an nPartition's processor configuration does not change, the correlations from physical processors to logical HP-UX processor IDs may change when HP-UX is rebooted in the nPartition.

This list gives details on how processors are available and numbered by HP-UX running on nPartitions.

- The following processors are *numbered* and are *available*: processors that are configured, reside on active cells, and (if HP's iCOD software is configured) are activated by iCOD.
- Processors that are *deconfigured* are not available and are not numbered by HP-UX.

  For deconfigured processors to be available they first must be configured using the nPartition's Boot Console Handler (BCH) interface.

  For details refer to the chapter *Listing and Managing Server Hardware* on page 305.
- Processors on *inactive cells* are not available and are not numbered by HP-UX. The cells must be active and must have configured processors in order to contribute processors to the nPartition.
- Processors that have been *deactivated* by HP's Instant Capacity on Demand (iCOD) software *are* numbered by HP-UX but are not available to be used until they are activated by iCOD.

  This means that when iCOD has deactivated one or more processors, some processors were numbered by are not listed in output displayed by commands such as `mpsched -s`, `top`, or `sar`.

  For example, the `mpsched` output below shows that processors 1, 2, 5, 6 and possibly others are deactivated. (To view more iCOD details use `icod_stat`.) Refer to the chapter *Processor Instant Capacity on Demand (iCOD)* on page 397 for details.

  ```
  # mpsched -s
  System Configuration
  =====================
  Locality Domain Count: 1
  ```

5377

```
Processor Count       : 5

Domain     Processors
------     ----------
0          0   3   4   7   8
#
```

The System Default Pset

When Pset software is installed, a *system default Pset* always exists that gives all users access to the processors assigned to it. The default Pset is Pset 0, which always has at least processor ID 0 assigned to it.

All processors are initially assigned to the default Pset until you configure processors to belong to other Psets.

When a Pset is destroyed or when a processor is removed from a Pset, the processors involved are assigned back to the default Pset.

Pset Attributes and Access Permissions

Each Pset has attributes that configure the Pset's behavior in various situations. These attributes also include "owner, group, and others" access permissions similar to traditional HP-UX file permissions. The default Pset's attributes cannot be changed, but all other Psets can have their attributes adjusted as needed.

Users who have write access for a Pset can modify *some* of the Pset's attributes, including attributes other than the access permissions. Each Pset's owner can modify the Pset's access permissions.

The following users can modify *all aspects* of all non-default Psets in a system: `root`, `superuser`, and users who belong to a group that has the `PSET` privileged capability. These users can modify all Pset attributes, modify all Pset processor assignments, and can create and destroy Psets.

The `PSET` privileged capability is established for a group by issuing the `setprivgrp` command. For example, `setprivgrp mygrp PSET` applies this privilege (and no other privileges) to the "mygrp" group. See the *setprivgrp* (1M) manpage for details.

Pset Boot-Time Configuration

When HP-UX boots on an nPartition that has Pset software installed, by default all processors are assigned to the default Pset: Pset 0.

You can have multiple Psets established at boot time either by creating HP-UX startup scripts that configure Psets, or by configuring Psets through PRM and having PRM establish configurations at boot time.

Pset Binding and Inheritance

Child threads and processes inherit the Pset bindings of their parents.

So, for example, when a process creates child processes, the children are are launched into the same Pset as the parent.

By using the Pset programming interface you can have more control over the Pset locations where threads and processes are spawned and run.

Using PRM on nPartitions with Psets

The HP Process Resource Manager product enables you to create and manage Psets through its graphical interface.

PRM provides the ability to maintain Pset configurations across system reboots. It also has the ability to assign (isolate) memory to Psets, thus giving Psets memory isolation as well as processor resource isolation.

PRM software refers to Psets that it tracks using PRM IDs or names, rather than using Pset IDs. PRM may modify Psets and cause them to be renumbered while managing Psets. Thus, if you use the `psrset -i` command while PRM has configured Psets, you may notice this renumbering of Pset IDs.

Note that if you have used PRM to assign specific processor IDs to Psets in the system, all specified processor IDs *must be present* for PRM to be able to load and establish the Pset configurations. Otherwise, when specified processors are not present, PRM cannot create the Psets.

You can help avoid this potential problem by not specifying processor IDs and instead specifying the *number of processors* for PRM to configure in each Pset.

This processor availability issue can prevent PRM from loading Pset configurations when iCOD software in an nPartition has *deactivated* one or more of the specified processors.

PRM also may be prevented from loading Pset configurations when any of the following has occurred in an nPartition: *deconfiguring* processors (at the BCH interface), *unassigning* a cell from an nPartition, or making one or more of an nPartition's cells *inactive*.

For details on managing PRM, see the PRM online help or *HP Process Resource Manager User's Guide*. Also see the *psrset* (1M) manpage for details on using the `-f` option while PRM is managing Psets.

Programming Interface for Psets

For details on the Pset programming interface, see the following HP-UX manpages: *pset_assign* (2), *pset_bind* (2), *pset_create* (2), *pset_ctl* (2), *pset_destroy* (2), *pset_getattr* (2), *pset_setattr* (2).

53>5

Tools for Managing and Using Psets

This section lists several tools for managing Psets.

For details, see these manpages: *psrset* (1M), *xprm* (1), *prmconfig* (1), *mpsched* (1), *rtsched* (1), *sar* (1M), *setprivgrp* (1M), and *getprivgrp* (1).

- `/usr/sbin/psrset`

  This command provides the main command-line interface for Psets.

- HP Process Resource Manager (PRM):
  `/opt/prm/bin/xprm` and
  `/opt/prm/bin/prmconfig`

  These commands provide graphical (`xprm`) and command-line (`prmconfig`) interfaces to PRM, which has built-in support for Psets.

- `/usr/bin/mpsched`

  This command provides a method for launching and managing time-share processes and threads, allowing for processor binding and unbinding, enabling gang scheduling, and inquiring about system and process attributes.

- `/usr/bin/rtsched`

  This command provides a method of launching real-time threads and processes.

- `/usr/sbin/sar`

  This command reports system activity, including Pset activity when the `-p` *`pset`* option or `-P` option is specified.

  For example, `sar -u -M -P 5` gives a snapshot of system processor use over a five second period, and because `-P` is specified Pset assignments are included.

- `/usr/sbin/setprivgrp` and
  `/usr/bin/getprivgrp`

  The `setprivgrp` command sets privileged capabilities for a specified group. When issuing this command, you must list all privileged capabilities that are to be applied for the group. For example: `setprivgrp mygrp PSET RTSCHED` grants special Pset and real-time scheduling capabilities to the members of the "mygrp" group.

To remove privileged capabilities for a group, issue the `setprivgrp` command with no capabilities specified (for example: `setprivgrp mygrp`).

The `getprivgrp` command reports privileged capabilities for the user issuing the command.

5373

Procedures for Managing Psets

This section lists only the psrset command-line procedures for managing Psets.

The common Pset tasks briefly given here are:

- *Listing Pset Configurations* on page 426
- *Creating a New Pset* on page 426
- *Destroying (Deleting) a Pset* on page 427
- *Assigning (Reassigning) Processors to Psets* on page 427
- *Unassigning (Removing) Processors from Psets* on page 427
- *Configuring Pset Attribute Values* on page 427
- *Setting Pset Access Permissions* on page 428
- *Running Programs in a Pset* on page 429
- *Binding Threads and Processes to a Pset* on page 429

Also see the *psrset* (1M) manpage for details, or see *Example Uses of Psets* on page 430 for command output and examples.

For details on support for Psets in HP Process Resource Manager (PRM) refer to the book *HP Process Resource Manager User's Guide* or the PRM online help.

Listing Pset Configurations

Step 1.

```
/usr/sbin/psrset -i
```

This lists all Psets defined in the system including the processors assigned to each and the owner, access permissions, and attributes for the Psets.

Creating a New Pset

Step 1.

```
/usr/sbin/psrset -c [processor_list]
```

where *processor_list* is an optional list of processors that are assigned to the newly created Pset.

S372

Destroying (Deleting) a Pset

Step 1.

```
/usr/sbin/psrset -d [pset_list | all]
```

where you specify either `all` (to delete all Psets) or a list of the Psets to be deleted (*`pset_list`*).

When you delete a Pset, the Pset's ID no longer exists and all processors assigned to the Pset are assigned to the default Pset. Deleting all Psets (`psrset -d all`) causes all processors to be assigned to the default Pset (Pset ID 0), which then is the only Pset in the system.

The user issuing this command must have write permission for the Psets that are deleted.

Assigning (Reassigning) Processors to Psets

Step 1.

```
/usr/sbin/psrset -a pset_id processor_list
```

where *`pset_id`* is the Pset to which the processors specified in *`processor_list`* are assigned.

The user issuing this command must have write permission for both the Pset specified by *`pset_id`* and the Pset(s) to which the processors in *`processor_list`* are assigned.

Unassigning (Removing) Processors from Psets

Step 1.

```
/usr/sbin/psrset -r processor_list
```

where *`processor_list`* is the list of processors that will be removed from their current Psets and assigned to the default Pset.

The user issuing this command must have write permission for the Pset(s) to which the processors in *`processor_list`* are assigned.

Configuring Pset Attribute Values

To configure access permissions (OWNID, GRPID, PERM) you must have root or superuser access or membership in a group that has PSET privileged capabilities.

537

You cannot modify attributes for Pset ID 0.

Step 1. `/usr/sbin/psrset -t pset_id attr_name=attr_value`

where *pset_id* is the Pset whose attribute(s) will be configured.

Each attribute (*attr_name*) is set to the corresponding value (*attr_value*) specified.

Attributes include OWNID, GRPID, PERM, and others listed in the *psrset* (1M) manpage.

Step 2. `/usr/sbin/psrset [-n | -F] pset_id`

where *pset_id* is the Pset for which external I/O interrupts are either enabled (-n) or disabled (-F).

When configuring attributes other than access permissions, the user issuing these commands must have write permission for the Psets specified.

Setting Pset Access Permissions

Step 1. Use the psrset command's -t option, as described in *Configuring Pset Attribute Values* on page 427.

To configure access permissions (OWNID, GRPID, PERM), you must have root or superuser access or membership in a group that has PSET privileged capabilities.

Specify the PERM attribute and corresponding value to set access permissions.

```
/usr/sbin/psrset -t pset_id PERM=p1p2p3
```

where *pset_id* is the Pset and *p1p2p3* is the set of access permissions for the Pset owner (*p1*), Pset group (*p2*), and others (*p3*).

Each access permission (owner, group, and others) is a number from 0–7 to indicate execute (x), write (w), and/or read (r) permissions.

0=no permissions, 1=x, 2=w, 3=xw, 4=r, 5=xr, 6=wr, 7=xwr

Execute allows running programs in the Pset, write allows changing the Pset configuration, and read allows reading the Pset configuration.

For example “PERM=754” gives the Pset owner execute, write, and read permissions; gives members of the Pset’s group execute and read permissions; and gives other users only read permission.

You also can specify attributes and values to change the owner (OWNID) and group (GRPID) for the Pset.

Running Programs in a Pset

Step 1. `/usr/sbin/psrset -e pset_id command [arguments]`

where *pset_id* is the Pset in which the specified *command* will be executed.

As needed, specify *arguments* to list any command-line options or arguments for the command.

The user issuing this command must have execute permission for the Pset in which the command is run.

Binding Threads and Processes to a Pset

Step 1. `/usr/sbin/psrset -b pset_id pid_list`

where *pset_id* is the Pset in which the specified process IDs (*pid_list*) will be bound.

The user issuing this command must have execute permission for both the original and new Psets in which the process ID executes.

Example Uses of Psets

NOTE

These examples show the use of processor sets (Psets) on an HP Superdome server that also has HP Instant Capacity on Demand (iCOD) “pay per use” software installed.

Uses of the optional HP iCOD software commands are noted in the text accompanying the examples.

For iCOD management information, refer to the chapter *Processor Instant Capacity on Demand (iCOD)* on page 397.

The following Pset examples are given in this section.

- *Listing, Creating, and Using Psets* on page 430
- *Destroying a Pset and Reassigning Processors* on page 432
- *Example of Running and Binding Programs in Psets* on page 434
- *Managing Pset Permissions and Attributes* on page 436

Example 10-1 Listing, Creating, and Using Psets

Initially this nPartition has only one Pset: the default Pset, which is Pset 0.

```
# psrset -i
PSET         0
SPU_LIST     0    1    2    3    4    5    6    7    8    9    10   11
OWNID        0
GRPID        0
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

#
```

S368

The icod_modify command sets the total number of processors to four. As the psrset -i command shows, this reduces the number of processors that are available and assigned to Psets. Note that processor IDs (listed in the SPU_LIST) are *not sequentially numbered* because several processors have been deactivated by the iCOD software.

```
# icod_modify -s 4 "set to 4":Ann:Joe:jdoe@comp.com:555-5555

4 processors are now active.

NOTE:    Verify that HP and 3rd party software licenses are upgraded
         to take into account the number of active processors.

# psrset -i
PSET         0
SPU_LIST     0     3     4     8
OWNID        0
GRPID        0
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

#
```

Create a new Pset using processor IDs 4 and 8, using the psrset -c... command. Then list all Psets using the psrset -i command.

```
# psrset -c 4 8
successfully created pset 2
successfully assigned processor 4 to pset 2
successfully assigned processor 8 to pset 2
# psrset -i
PSET         0
SPU_LIST     0     3
OWNID        0
GRPID        0
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

PSET         2
SPU_LIST     4     8
OWNID        0
GRPID        3
PERM         755
IOINTR       ALLOW
```

536

```
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

#
```

Example 10-2 Destroying a Pset and Reassigning Processors

List the local nPartition's Pset configuration using the `psrset -i` command. There are three Psets: the default Pset 0, Pset 10, and Pset 11.

```
# psrset -i
PSET         0
SPU_LIST     0     1     2     3     4
OWNID        0
GRPID        0
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

PSET         10
SPU_LIST     9     10    11
OWNID        0
GRPID        3
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

PSET         11
SPU_LIST     5     6     7     8
OWNID        0
GRPID        3
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

#
```

Destroy Pset 10 because it is no longer needed. Its processors (9, 10, and 11) are assigned back to the default processor set (Pset 0). Then list the new Pset configurations using the `psrset -i` command.

5366

```
# psrset -d 10
successfully destroyed pset 10
# psrset -i
PSET         0
SPU_LIST     0    1    2    3    4    9    10   11
OWNID        0
GRPID        0
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

PSET         11
SPU_LIST     5    6    7    8
OWNID        0
GRPID        3
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

#
```

Assign processors 4 and 9 to Pset 11 using the `psrset -a...` command. Then list the new Pset configurations using `psrset -i`, which shows the processor assignments for all Psets (Pset 0 and Pset 11).

```
# psrset -a 11 4 9
successfully assigned processor 4 to pset 11
successfully assigned processor 9 to pset 11
# psrset -i
PSET         0
SPU_LIST     0    1    2    3    10   11
OWNID        0
GRPID        0
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

PSET         11
SPU_LIST     4    5    6    7    8    9
OWNID        0
GRPID        3
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
```

5365

```
LASTSPU      DFLTPSET

#
```

Example 10-3 Example of Running and Binding Programs in Psets

List the current Pset configuration for the local nPartition. Two Psets are configured: Pset 0 and Pset 2.

Note that processor ID 10 is not active in this nPartition (because iCOD software has deactivated it).

```
# psrset -i
PSET         0
SPU_LIST     0    2    9
OWNID        0
GRPID        0
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

PSET         2
SPU_LIST     1    3    4    5    6    7    8    11
OWNID        0
GRPID        3
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

#
```

Use the mpsched command to run the “potato” program and bind it to processor ID 2. Then use the psrset -q... command to list the Pset binding for “potato” (process ID 10368); “potato” is bound to Pset 0.

```
# mpsched -c 2 ./potato -n 7
Pid 10368: bound to processor 2 using the default process launch policy
Threads = 7
tid = 2  cpu = 2
tid = 3  cpu = 2
tid = 4  cpu = 2
tid = 5  cpu = 2
tid = 6  cpu = 2
tid = 7  cpu = 2
tid = 1  cpu = 2
```

```
# psrset -q 10368
PID  10368         PSET  0
#
```

Use the psrset -b... command to change the Pset binding for “potato” to Pset 2. Then use psrset -q... to confirm that it is bound to Pset 2, and use the mpsched -q... command to check its processor binding.

```
# psrset -b 2 10368
successfully bound pid 10368 to pset 2
# psrset -q 10368
PID  10368         PSET  2
# mpsched -q -p 10368
Pid 10368: bound to processor 3 using the default process launch policy
#
```

Use the sar command to list the current nPartition’s processor usage, including Pset details. Note that processor ID 3 in (Pset 2) is heavily loaded by the “potato” program.

```
# sar -u -M -P 1

HP-UX feshd5a B.11.11 U 9000/800    10/23/01

00:17:11    pset     cpu    %usr    %sys    %wio   %idle
00:17:12       0       0       0       0       7      92
               2       1       0       0      10      90
               0       2       0       0       8      92
               2       3     100       0       0       0
               2       4       0       0       4      96
               2       5       0       0       8      92
               2       6       0       0       7      93
               2       7       0       0       9      91
               2       8       0       0       5      95
               0       9       0       1       9      90
               2      11       0       0       8      92
                  system       9       0       7      84
#
```

Use the mpsched -u... command to *unbind* the “potato” program (process ID 10368) from processor ID 3, to allow the program’s threads to migrate to other processors in the Pset to which it is bound.

Then use sar to list the local nPartition’s current processor usage, including all processor and Pset details.

Since the “potato” program was unbound from processor 3, its threads were able to migrate to the other processors in the Pset to which it “potato” is bound (Pset 2).

S363

All processors in Pset 2 are being used fairly heavily, while processors in Pset 0 are 100% idle. This is due to Pset processor resource isolation: by default each program only uses processors in the Pset in which it is run. (The Pset programming interface can override this default to launch threads and processes in other Psets, given the right conditions.)

```
# mpsched -u -p 10368
Pid 10368: not bound using the default process launch policy
# sar -u -M -P 1

HP-UX feshd5a B.11.11 U 9000/800    10/23/01

00:24:26     pset     cpu     %usr     %sys     %wio    %idle
00:24:27        0       0        0        0        0      100
                2       1      101        0        0        0
                0       2        1        0        0      100
                2       3      101        0        0        0
                2       4      100        1        0        0
                2       5       96        0        0        5
                2       6      101        0        0        0
                2       7      101        0        0        0
                2       8       18        2        0       81
                0       9        0        1        0      100
                2      11       88        0        0       13
                    system      64        0        0       36

#
```

Example 10-4 Managing Pset Permissions and Attributes

This example modifies Pset owner, group, and access permissions; lists various Pset details; and includes other sample Pset uses by various users on the system.

Use psrset -i to list the current Pset configuration for the local nPartition. Three Psets are configured: Pset 0, Pset 7, and Pset 8.

```
# psrset -i
PSET         0
SPU_LIST     0    1    2    3    4    5
OWNID        0
GRPID        0
PERM         755
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET
```

5362
21

```
PSET          7
SPU_LIST      9     10    11
OWNID         0
GRPID         3
PERM          755
IOINTR        ALLOW
NONEMPTY      DFLTPSET
EMPTY         FAIL
LASTSPU       DFLTPSET

PSET          8
SPU_LIST      6     7     8
OWNID         0
GRPID         3
PERM          755
IOINTR        ALLOW
NONEMPTY      DFLTPSET
EMPTY         FAIL
LASTSPU       DFLTPSET

#
```

Modify the group setting for Pset 8 to be group ID 20. Also use `psrset -t...` to modify the permissions for Pset 8. Setting the permissions to 774 allows the owner (`root`) and users in group ID 20 (the group named `users`) to execute, write, and read Pset 8; all others can only read details about the Pset's configuration.

```
# psrset -t 8 GRPID=20
# psrset -t 8 PERM=774
#
```

Using the `psrset -t...` command, change the owner for Pset 7 to user ID 103 (the user named ann).

```
# psrset -t 7 OWNID=103
#
```

Now ann uses the `id` command to list the user ID and group memberships for her user account. She then lists the current Pset configuration for the local nPartition.

The ann user account gives her execute and read access to Pset 0, ownership of Pset 7 (including execute, write, and read access), and execute, write, and read access for Pset 8.

She (ann) is considered one of the "others" (access permissions 5) for Pset 0, the owner (user ID 103, with access permissions 7) for Pset 7, and a group member (group ID 20, access permission 7) for Pset 8.

S361

```
ann $ id
uid=103(ann) gid=20(users) groups=102(prog)
ann $ psrset -i
PSET        0
SPU_LIST    0    1    2    3    4    5
OWNID       0
GRPID       0
PERM        755
IOINTR      ALLOW
NONEMPTY    DFLTPSET
EMPTY       FAIL
LASTSPU     DFLTPSET

PSET        7
SPU_LIST    9    10   11
OWNID       103
GRPID       3
PERM        755
IOINTR      ALLOW
NONEMPTY    DFLTPSET
EMPTY       FAIL
LASTSPU     DFLTPSET

PSET        8
SPU_LIST    6    7    8
OWNID       0
GRPID       20
PERM        774
IOINTR      ALLOW
NONEMPTY    DFLTPSET
EMPTY       FAIL
LASTSPU     DFLTPSET

ann $
```

Because ann is the owner for Pset 7, she has authority to modify the Pset's user, group, and access permissions attributes.

Using the `psrset -t...` command, ann sets the group for Pset 7 to 102 (the group named prog). Another `psrset -t...` command sets access permissions for Pset 7 to 770, which gives the owner (ann) and prog group members access to execute, write, and read the Pset. All others have no permissions to use or read Pset 7.

```
ann $ psrset -t 7 GRPID=102
ann $ psrset -t 7 PERM=770
ann $
```

Now ann assigns processor ID 8 to Pset 7, using the `psrset -a...` command.

Processor 8 was assigned to Pset 8, but ann can reassign it because she has write permission for Pset 8 (she is a member of group ID 20, which has execute, write, and read permissions).

Likewise, ann can assign the processor to Pset 7 because she has write permissions there (she is the owner, and has execute, write, and read permissions).

Then ann lists the new configurations for Pset 7 and Pset 8 using the `psrset -i 7 8` command.

```
ann $ psrset -a 7 8
successfully assigned processor 8 to pset 7
ann $ psrset -i 7 8
PSET         7
SPU_LIST     8     9     10    11
OWNID        103
GRPID        102
PERM         770
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

PSET         8
SPU_LIST     6     7
OWNID        0
GRPID        20
PERM         774
IOINTR       ALLOW
NONEMPTY     DFLTPSET
EMPTY        FAIL
LASTSPU      DFLTPSET

ann $
```

Now a different user in the same nPartition attempts to list and use the new Pset configurations.

This user, `joe`, lists his user ID and the IDs for the groups to which he belongs, and then lists all Pset configurations using the `psrset -i` command. Note that because `joe` does not have read permission for Pset 7, he cannot view its attribute values (he is not the owner or a member of the Pset's group, so as one of the "others" he has no permissions).

535a

```
joe $ id
uid=102(joe) gid=20(users)
joe $ psrset -i
PSET          0
SPU_LIST      0     1     2     3     4     5
OWNID         0
GRPID         0
PERM          755
IOINTR        ALLOW
NONEMPTY      DFLTPSET
EMPTY         FAIL
LASTSPU       DFLTPSET

PSET          7
SPU_LIST      8     9     10    11
psrset: no privileges for query operation on this pset

PSET          8
SPU_LIST      6     7
OWNID         0
GRPID         20
PERM          774
IOINTR        ALLOW
NONEMPTY      DFLTPSET
EMPTY         FAIL
LASTSPU       DFLTPSET

joe $
```

When `joe` uses the `psrset -e 7...` command to attempt to execute the “potato” program in Pset 7, he cannot because he does not have execute permission in the Pset.

However, when `joe` uses the `psrset -e 8...` command to execute “potato” in Pset 8 the program is run in that Pset. He can run programs in Pset 8 because he is a member of group ID 20 and members of that group have execute, write, and read permission for the Pset.

```
joe $ psrset -e 7 ./potato
psrset: no privileges to perform operation
joe $ psrset -e 8 ./potato
Threads = 2
tid = 1  cpu = 6
tid = 2  cpu = 7
...
```

S358

11 Virtual Partitions (vPars) Management on nPartitions

This chapter describes how to create, configure, and manage HP's virtual partitions within an nPartition (hard partition) system environment. Each virtual partition can boot a single instance of the HP-UX B.11.11 operating system.

The HP **virtual partitions (vPars)** software is an *optional* feature that you can use to further subdivide a server's resources into multiple, smaller virtual machines through software partitioning.

By configuring multiple virtual partitions within an nPartition, you can boot multiple instances of HP-UX B.11.11 in a single nPartition.

For detailed tasks for configuring virtual partitions within an nPartition, see *Procedures for Managing Virtual Partitions on HP nPartition Servers* on page 475.

NOTE This chapter describes the current A.02.02 vPars software release, which supports HP rp7405/rp7410, HP rp8400, and HP Superdome servers.

For an introduction to nPartition features, refer to the chapter *nPartition System Overviews* on page 31.

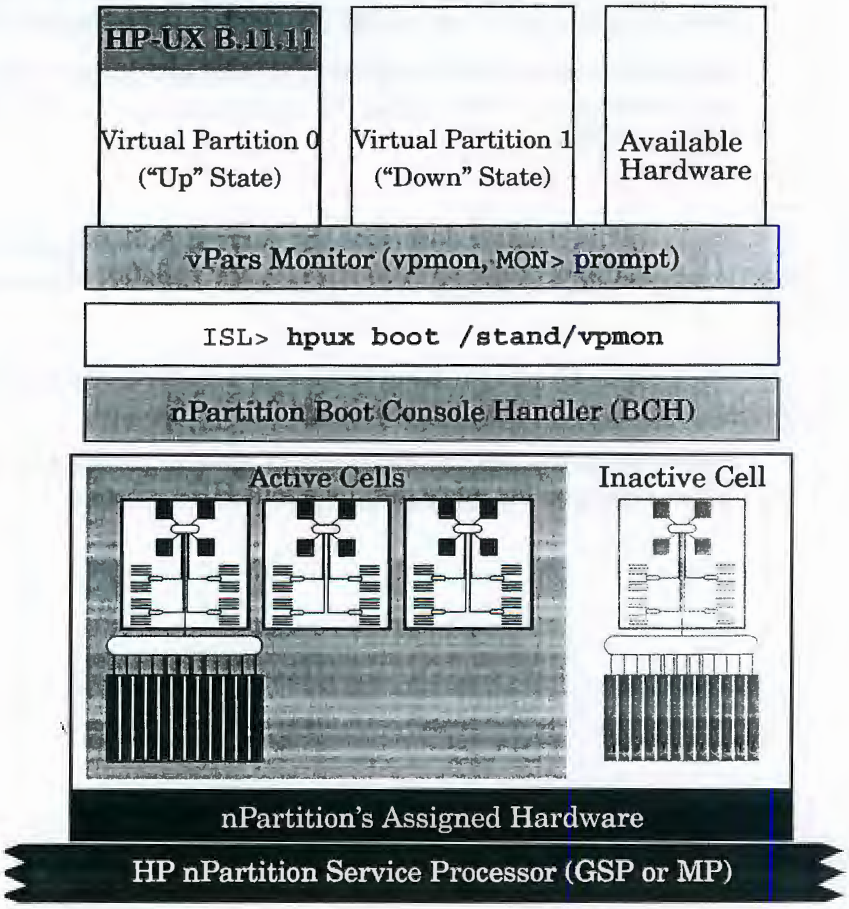
Also refer to the book *Installing and Managing HP-UX Virtual Partitions (vPars)* for more details about HP's vPars software.

S33

Introduction to Managing Virtual Partitions on nPartitions

Figure 11-1 shows how an nPartition can boot vPars software from its BCH interface, thus enabling one or more virtual partitions to run HP-UX B.11.11 on a subset of the nPartition's active hardware.

Figure 11-1 **Overview of HP Virtual Partitions (vPars) in an nPartition**


HP-UX B.11.11
Virtual Partition 0
("Up" State)
Virtual Partition 1
("Down" State)
Available Hardware
vPars Monitor (vpmon, MON> prompt)
ISL> hpux boot /stand/vpmon
nPartition Boot Console Handler (BCH)
Active Cells
Inactive Cell
nPartition's Assigned Hardware
HP nPartition Service Processor (GSP or MP)

Virtual Partition Hardware

On HP nPartition servers, each virtual partition is assigned a subset of its nPartition's hardware. Only the *active hardware assigned to the local nPartition* can be used by virtual partitions within the nPartition.

Hardware that is assigned to remote nPartitions and hardware that is inactive cannot be used by virtual partitions in the local nPartition.

Each virtual partition runs its own instance of HP-UX and has its own dedicated hardware resources. You can reconfigure virtual partitions and can dynamically reallocate certain processors among virtual partitions in the local nPartition, but you cannot share resources across virtual partitions or across nPartitions.

The hardware assigned to each virtual partition includes: processors (CPUs), memory, and input/output busses. Each I/O bus can have a PCI card installed and devices attached.

Each virtual partition should be assigned at least one I/O bus (LBA) that has a boot device with HP-UX B.11.11 and the vPars software product installed. An I/O bus with a network interface card also should be assigned to each virtual partition to support networking. See *vPars Requirements and Recommendations* on page 454 for more details.

vPars Software, Booting, and Consoles

Running virtual partitions in an nPartition involves installing the HP-UX virtual partitions software product, configuring one or more virtual partitions, and then booting the vPars monitor (`/stand/vpmon`) on the nPartition and loading/booting HP-UX on each of the virtual partitions.

By booting the `/stand/vpmon` virtual partitions monitor instead of the `/stand/vmunix` HP-UX kernel, an nPartition provides an additional boot loader specifically for virtual partitions.

Each nPartition can be configured to automatically boot virtual partitions, and virtual partitions can individually be configured to be booted manually or automatically. See *Procedures for Managing Virtual Partitions on HP nPartition Servers* on page 475 for details.

Only one vPars monitor is booted per nPartition. All virtual partitions in an nPartition share the same console device: the nPartition's console. See *Virtual Partition Console and Log Use on nPartition Servers* on page 465 for details.

5355

vPars HP-UX B.11.11 Kernel

The vPars software installation builds a relocatable, vPars-enabled HP-UX B.11.11 kernel and installs patches, commands, and vpmon to support the vPars software environment. See *Installing and Configuring vPars on nPartition Servers* on page 472 for details.

You can load and run a vPars-enabled HP-UX B.11.11 kernel in both vPars environments and non-vPars environments. You *do not* need to reconfigure a vPars-enabled kernel for non-vPars use.

nPartition and vPars Performance

In general in HP nPartition virtual partitions environments, HP-UX B.11.11 and application *performance is nearly equivalent* to the performance given by a non-vPars nPartition that has the same hardware and software resources and configuration.

Also see the document *HP-UX Virtual Partitions Ordering and Configuration Guide* for more virtual partitions performance info.

The main performance factor for virtual partitions running in nPartitions is the underlying nPartition's hardware configuration: the cells and corresponding processors, memory, and I/O assigned to and actively used in the nPartition.

As in non-vPars nPartition environments, all memory is interleaved across all active cells in the nPartition when virtual partitions are running in an nPartition. Also on all HP nPartition servers, each processor has its own runway bus for communication to memory and I/O.

As a result, the locations (hardware paths) of processors assigned to a virtual partition *do not* affect performance. In general all processors have the same memory latency when accessing any significant amount of memory in an nPartition.

The rest of this chapter covers requirements, guidelines, procedures, and tools for using virtual partitions on HP nPartition-capable servers.

5354

Configuring Virtual Partition Resources and Attributes

When creating or reconfiguring a virtual partition, you manage **resources and attributes** that determine the virtual partition's configuration and capabilities.

Each virtual partition has three types of resources: `cpu`, `io`, and `mem`, which specify processor(s), I/O, and memory allocated exclusively for the virtual partition.

The virtual partition resource configuration determines which hardware is dedicated for the virtual partition's use, by indicating hardware paths, quantities, and limits.

Each virtual partition also has three types of attributes: general attributes, hardware attributes, and boot attributes.

NOTE To modify most virtual partition *hardware* resources or attributes, you must ensure that the virtual partition being modified is in a "Down" state.

Also note that some virtual partition attributes are required and some are optional.

See the *vparmodify* (1M) and *vparresources* (5) manpages for details.

The following list includes details and command-line options for setting virtual partition attributes. Also see the *vparcreate* (1M) and *vparmodify* (1M) command manpages.

- **Virtual Partition General Attributes**

  The **general virtual partition attributes** include the *name* of the virtual partition and the `static` attribute.

  The *name* attribute (`-p` and `-P`) defines the virtual partition's name, which you use when referencing or managing the virtual partition using commands.

5353

The *static* attribute (-S) defines whether the virtual partition can be reconfigured. See *Dynamic and Static Virtual Partitions* on page 461 for details.

- **Virtual Partition Hardware Resource Attributes**

  Virtual partition hardware resource attributes include specifications for the processors, I/O, and memory that are dedicated for use by the virtual partition.

  You can add (-a), delete (-d), and modify (-m) virtual partition hardware resources and attributes.

  Also see the *vparresources* (5) manpage for details.

  Descriptions of processor (cpu), I/O (io), and memory (mem) virtual partition hardware resource attributes are in the following list.

  — Processors (cpu) resources — You can specify the following attributes for processors:

  The *path* of one or more processors that are bound to the virtual partition. For example, to set the processor at hardware path 0/10 to be bound to the virtual partition:

  ```
  # vparmodify -p name -m cpu:0/10
  ```

  A *minimum* and *maximum* number of processors allowed in the virtual partition. For example, to set the minimum number of processors to 2 and the maximum to 4 processors:

  ```
  # vparmodify -p name -m cpu:::2:4
  ```

  The *total* number of processors in the virtual partition. For example, to set the total number of processors to 6:

  ```
  # vparmodify -p name -m cpu::6
  ```

  — Input/Output (io) — You can optionally specify boot, altboot, and other attributes for each I/O device path assigned to a virtual partition.

  The boot attribute specifies the primary (PRI) boot device path for the virtual partition, which is stored in the vPars database (vpdb) and is separate from the nPartition boot device path settings.

The altboot attribute specifies the alternate (ALT) boot device path for the virtual partition, which also is separate from nPartition boot settings.

For example, to set the specified virtual partition's PRI boot device path to 0/0/6/0/0.5 (the corresponding nPartition's PRI path is *not* changed, however):

```
# vparmodify -p name -m io:0/0/6/0/0.5:boot
```

— Memory (mem) — You can specify the total (-m mem::*size*) memory *size* in MBytes for a virtual partition, and can increase (-a) or decrease (-d) the amount of memory,

As needed, the specified *size* is rounded up to a 64 MByte boundary.

For example, to configure a virtual partition to have 2 GBytes (2048 MBytes) of memory allocated:

```
# vparmodify -p name -m mem::2048
```

NOTE

HP recommends that you *only specify the total amount of memory* to be allocated for each virtual partition. On all supported HP virtual partition systems there is no benefit to specifying the base and range for memory.

Each nPartition's memory is interleaved across all active cells in the nPartition and thus all useful ranges of virtual partition memory will span all cells.

- **Virtual Partition Boot Attributes**

  Virtual partition boot attributes include the *autoboot* setting, the *kernel path* attribute, the *boot options* attribute, and *io resources* attributes.

  The *autoboot* attribute (-B) determines whether a virtual partition is booted (-B auto) or not booted (-B manual) when the virtual partition is reset. This attribute also affects virtual partition boot behavior when the vPars monitor is loaded with the vpmon -a option or when the vparload -auto command is issued from the MON> prompt.

The *`kernel path`* attribute (`-b`) specifies the path of the vPars-enabled HP-UX B.11.11 kernel that is to be booted when the virtual partition is loaded. By default the `/stand/vmunix` kernel on the boot device is used.

The *`boot options`* attribute (`-o`) specifies the options that are applied when the virtual partition's HP-UX B.11.11 kernel is booted. These boot options are equivalent to the secondary system loader options described in the *hpux* (1M) manpage.

You can use the *`io resources`* attributes (`-a io...`, `-m io...`) to designate primary (PRI) and alternate (ALT) boot device paths for a virtual partition, as explained in *Virtual Partition Hardware Resource Attributes* on page 446.

5350

Tools for Managing Virtual Partitions on nPartition Servers

The main tools for virtual partitions administration are the HP-UX vPars commands and the Virtual Partition Manager (`vparmgr`) utility.

This section briefly lists these and other tools and commands you can use for managing virtual partitions on HP nPartition servers.

- **HP-UX Virtual Partitions Commands**

  The HP-UX vPars commands create, modify, and provide status and configuration info about the virtual partitions in the *currently active* vPars database (`/stand/vpdb`), or any other accessible vPars database that you specify.

  The vPars commands list status or modify configuration details for virtual partitions in the local nPartition. They cannot modify or list info about virtual partitions running in remote nPartitions.

  Using all vPars commands requires `root` permission.

  In most cases the vPars commands are used after you have booted one or more virtual partitions in an nPartition. However, you also can use some vPars commands when you have booted HP-UX in a non-vPars nPartition environment, such as when initially configuring virtual partitions.

  See the *vpartition* (5) manpage for a list and descriptions of the vPars commands, including `vparstatus`, `vparcreate`, `vparmodify`, `vparboot`, `vparreset`, and others.

- **Virtual Partition Manager (`vparmgr`) Utility**

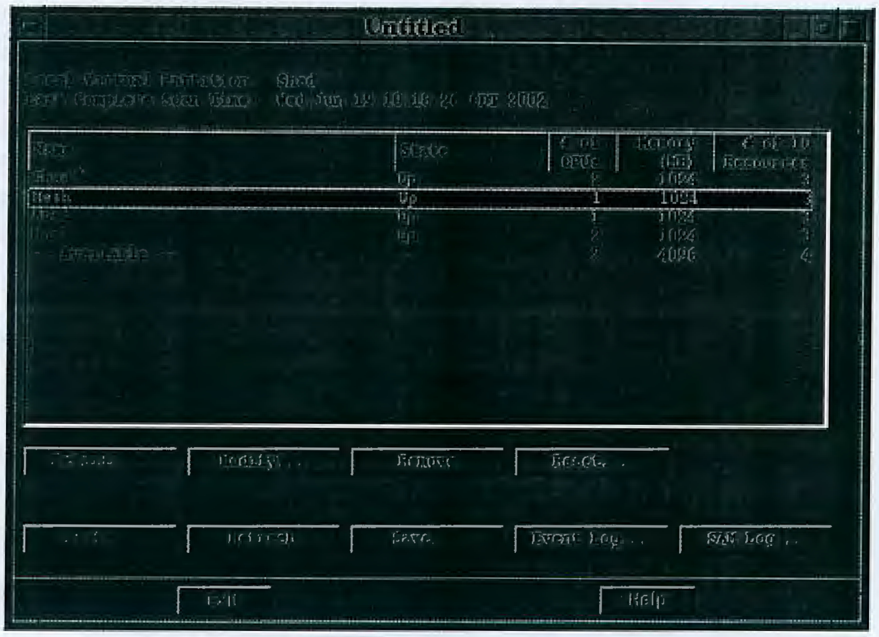
  The Virtual Partition Manager utility provides a graphical interface to the HP-UX vPars commands. Using Virtual Partition Manager, you can perform virtual partitions administration tasks from HP-UX running on a virtual partition. You cannot use Virtual Partition Manager when HP-UX is booted in non-vPars mode.

NOTE The Virtual Partition Manager utility *is not installed* as part of the virtual partitions software product installation. Instead, you must install Virtual Partition Manager separately, as described in the the book *Installing and Managing HP-UX Virtual Partitions (vPars)*.

Using the Virtual Partition Manager utility requires `root` permission.

Because Virtual Partition Manager is an X window graphical utility, you must set and export the virtual partition system's DISPLAY environment variable before launching `vparmgr`. The DISPLAY variable specifies where (which X server) the system displays X windows. You also must use the `xhost` command on the X server (your local system) to grant access for the virtual partition system to display windows on the X server. See the *X* (1) and *xhost* (1) manpages for details.

The following window is the Virtual Partition Manager utility's status window, which is the first window displayed after any alert messages. This window lists the status of all virtual partitions defined in the current vPars database as well as general details about available resources.



```
Untitled

Local Virtual Partition:    Shad
Last Complete Scan Time:    Wed Jun 19 10:16:20 EDT 2002

Name                     State     # of    Memory   # of IO
                                   CPUs    (MB)     Resources
Shad*                    Up          2     1024          3
Heth                     Up          1     1024          3
[illegible]              Up          1     1024          3
[illegible]              Up          2     1024          3
 -- Available --                     2     4096          4
```

Virtual Partition Manager has online help that you can view at any time by clicking the **Help** button, which displays info in a separate Web browser. You also can view Virtual Partition Manager help from a Web browser by issuing the following command:

```
/opt/netscape/netscape file:/opt/webadmin/vparmgr/help/C/overview.html
```

See the online help for complete details on using the Virtual Partition Manager.

All Virtual Partition Manager tasks also can be performed using the HP-UX vPars commands, which are described in the *vpartition* (5) manpage.

- HP-UX nPartition Commands: parstatus and Others

  The parstatus command can list nPartition status info as well as details about hardware assigned to the local nPartition and other hardware throughout the entire nPartition server complex.

  See the *parstatus* (1) manpage for details.

  The other HP-UX nPartition commands, such as parmodify, also are supported when running HP-UX in a virtual partition on an nPartition. Likewise the Partition Manager tool is supported.

3342

- HP-UX `setboot` Command

  The HP-UX `setboot` command affects the current virtual partition's boot settings (stored in its `/stand/vpdb`) when you use it in a virtual partition environment.

  When used in a *non-vPars* nPartition environment, the `setboot` command affects the local nPartition's boot settings. The nPartition boot device paths are stored in the nPartition's Partition Configuration Data portion of the server's Complex Profile.

- Tools for Boot Device AUTO File Management

  HP-UX commands to set (`mkboot`) and list (`lifcp`) a device's AUTO file: **`mkboot -a`** ***`STRING`*** **`/dev/dsk/...`** and **`lifcp /dev/dsk/...:AUTO -`**

  ISL commands to list (`hpux show...`) and set (`hpux set...`) an AUTO file: **`hpux show autofile`** and **`hpux set autofile`** ***`STRING`***

  vPars monitor (`MON>`) command to list an AUTO file: **`getauto`**

  See the *mkboot* (1M), *lifcp* (1), and *hpux* (1M) manpages.

- HP nPartition Virtual Front Panel (VFP)

  The nPartition VFP indicates the boot status for all cells and virtual partitions in the nPartition. As long as at least one virtual partition is running HP-UX the VFP will display an HP-UX "heartbeat".

  For details, refer to the chapter *Using Console and Service Processor Interfaces* on page 125.

- HP nPartition Console and Virtual Partition Consoles

  Each nPartition console provides access to BCH for the nPartition, allows you to boot HP-UX or the vPars monitor on an nPartition, and permits access to all virtual partition console interfaces in the nPartition.

  For details, see *Virtual Partition Console and Log Use on nPartition Servers* on page 465.

- HP vPars Monitor (`vpmon`) Commands

  At the vPars monitor (`MON>`) prompt enter **`?`** or the **`help`** command to list all available vPars monitor commands.

5346

The vPars monitor commands include: `reboot` (reboot the nPartition), `vparload` (load/boot one or more virtual partitions), `scan` (scan and list all active hardware in the local nPartition), `log` (list recent history from the vPars monitor's event log), and other commands.

The vPars monitor's `MON>` prompt is available when the nPartition's monarch processor is not assigned to a virtual partition that has been loaded/booted.

- HP nPartition Service Processor (GSP or MP) Commands

  Service processor commands that reboot or reset an nPartition affect all virtual partitions within the nPartition.

  For details, refer to the chapter *Using Console and Service Processor Interfaces* on page 125.

- HP nPartition Server Chassis Log Viewer (SL)

  HP virtual partitions-related details that are accessible as chassis logs include the HP-UX "heartbeat" emitted when HP-UX is running on each virtual partition. Otherwise, all vPars-specific event logs are stored in the vPars event log.

  For details, see the section *Virtual Partition Console and Log Use on nPartition Servers* on page 465.

5345

vPars Requirements and Recommendations

HP offers the following requirements and recommendations for configuring virtual partitions in HP nPartition environments.

Additional recommendations for avoiding obstacles to loading/booting virtual partitions are in *Fault-Tolerant Virtual Partition Configurations for nPartitions* on page 457.

NOTE See the *HP-UX Virtual Partitions Ordering and Configuration Guide* for the latest requirements.

Configuration Requirements and Recommendations for Virtual Partitions

❑ The following software releases, or later, **must** be installed for complete vPars support on HP nPartition-capable servers:

— Any HP-UX B.11.11 release (December 2000 or later).

— The A.02.02 virtual partitions software product.

— The Partition Manager B.11.11.01.05 product, which must be installed *before* the A.02.02 vPars software is installed.

— The Superdome SMS Software V1.2 release (including firmware).

❑ Each nPartition in which virtual partitions are configured **must** have *no more than* eight cells assigned to it, and all the nPartition's cells **must** reside in the same cabinet.

❑ Each nPartition **must** have *no more than* eight virtual partitions configured.

If you require more than eight virtual partitions in the same HP nPartition complex, configure the virtual partitions in multiple nPartitions.

❑ Hardware to be used by virtual partitions within an nPartition **must** be *assigned* to the local nPartition and must be *active* hardware.

Because each nPartition only provides access to the hardware that is assigned to and active within the local nPartition, any virtual partitions in the nPartition are limited to using this same set of currently available nPartition hardware.

Adding or removing hardware from an nPartition changes the local set of hardware that is available to virtual partitions in the nPartition. Likewise, making nPartition hardware inactive makes it unavailable to virtual partitions.

- ❑ At least one processor **must** be bound to each virtual partition.

  Only bound processors can handle I/O interrupts. Other processors in the virtual partition can be either bound or unbound.

- ❑ A multiple of 64 MBytes of memory **must** be assigned to each virtual partition.

  When you specify the memory size of each virtual partition, the commands involved automatically round the memory assignment upward as required to a 64-MByte boundary.

  Memory in HP nPartitions is interleaved across all active cells in the local nPartition. As a result the memory used by each virtual partition may physically reside on all active cells in the nPartition where the virtual partitions exist.

- ❑ Each virtual partition **must** have at *least one* I/O bus (LBA) assigned to it.

  On HP nPartition servers, each LBA corresponds to a PCI card slot in an I/O chassis attached to an active cell in the local nPartition.

  For I/O slot details, see the section *Planning Virtual Partition Configurations for HP nPartition Servers* on page 467.

- ❑ Each virtual partition **must** have at least one bootable disk accessible through a PCI card in one of the I/O busses assigned to the virtual partition.

  The bootable disk must have both HP-UX B.11.11 and the HP virtual partitions software package installed.

- ❑ The HP processor pay per use (PPU, or iCOD Utility) product is *not yet supported for virtual partitions* and **must not** be installed or configured for nPartition systems running vPars.

5343

The HP processor Instant Capacity on Demand (iCOD Purchase) release B.05.00 software may be installed and used with vPars software on HP nPartition-capable servers.

A future release of iCOD Utility (pay per use) also will support processor capacity on demand for nPartition servers running vPars.

□ Each virtual partition **should** have at least one LAN card or port available through one of the I/O busses assigned to the virtual partition.

The LAN port is required if HP-UX networking is to be supported.

HP recommends that, for best performance, you do not configure HP-UX lan0 to use the nPartition's Core I/O LAN (on HP Superdome servers, the LAN at hardware path *cell*`/0/0/1/0`).

The HP Superdome Core I/O card is a PCI-1x card that possibly provides lower performance than a comparable PCI-2x or PCI-4x card.

□ If you require that a virtual partition not be reconfigured then you **should** set the virtual partition to be "static". For details, see *Dynamic and Static Virtual Partitions* on page 461.

The next section gives detailed guidelines for creating fault-tolerant virtual partition configurations on nPartitions.

5338

Dynamic and Static Virtual Partitions

Each virtual partition has a static/dynamic attribute that determines whether resource changes can be made to the virtual partition.

A **static virtual partition** cannot have any modifications made to its resource profile. This means that the virtual partition's processor, memory, and I/O characteristics and assignments cannot be changed, even if the virtual partition is not running (in a "Down" state).

A **dynamic virtual partition** can have its resource profile changed through the use of the `vparmodify` command.

To toggle between the `static` and `dynamic` virtual partition attribute settings, use the `vparmodify` command's `-S` option:

```
vparmodify -p vpname -S static
```

```
vparmodify -p vpname -S dynamic
```

You also can toggle this attribute between `dynamic` and `static` in a single command. For example, the following command sets the virtual partition named "Shad" to be dynamic, then modifies its total number of CPUs, then sets the virtual partition to be static.

```
# vparmodify -p Shad -S dynamic -m cpu::3 -S static
```

See the *vparmodify* (1M) manpage for details.

Note that some resource changes require that the virtual partition not only be dynamic but also be in a "Down" state.

For example, changing I/O attributes or adding and removing processors may be possible while a dynamic virtual partition is running, but changing memory or I/O assignments requires a virtual partition to be both *dynamic* and *down*.

To check virtual partition static/dynamic attribute settings, use `vparstatus`.

```
# vparstatus
[Virtual Partition]
                                                                    Boot
Virtual Partition Name            State Attributes Kernel Path              Opts
============================== ===== ========== ========================= =====
Shad                              Down  Dyn,Manl   /stand/vmunix
Mesh                              Up    Stat,Manl  /stand/vmunix            boot
```

```
[Virtual Partition Resource Summary]
                                                     CPU     Num        Memory (MB)
                                            CPU    Bound/    IO    # Ranges/
Virtual Partition Name                    Min/Max  Unbound  devs   Total MB     Total MB
==============================            ================  ====   ====================
Shad                                        2/  8     2    0    8     0/   0        2048
Mesh                                        2/ 12     2    6    3     0/   0        2048
# vparmodify -p Mesh -m cpu::4
vparmodify: Error: Virtual partition Mesh is static, cannot modify resources.
#
```

5336

Virtual Partition Configuration Data on nPartitions

This section covers configuration data issues related to using virtual partitions in nPartitions.

Virtual partition configuration data by default is stored in the `/stand/vpdb` file, although you can specify that another file be used as the vPars database.

When you have multiple virtual partitions booted (in an "Up" state) on an nPartition, the vPars databases for all booted virtual partitions are kept coherent; any changes to virtual partition configurations are saved in each of the booted virtual partition's databases.

Virtual partition configuration data *is not* stored in the nPartition complex profile data. As a result, virtual partition changes do not affect nPartition configurations.

The following list describes some issues related to managing both nPartition and virtual partitions configuration data in an nPartition.

- Boot Paths for Virtual Partitions and nPartitions

  Each nPartition's boot path variables (PRI, HAA, ALT) are stored in the nPartition's profile data.

  The virtual partition boot device paths (PRI, ALT) are stored in the vPars configuration database.

  The `parmodify` and `parstatus` commands always can report and modify nPartition boot device path details.

  When one or more virtual partitions is booted in an nPartition, the `setboot` command affects the *current virtual partition's* boot paths and settings.

  When HP-UX is booted in a *non-vPars nPartition*, the `setboot` command and others affect the local nPartition.

- Virtual Partition Configuration Data Coherency

  Only the vPars configuration database (`/stand/vpdb`) residing on each virtual partition's currently booted device's filesystems is updated to reflect any changes.

Any booted virtual partition that has multiple boot devices (such as `boot` and `altboot`) can have one current and one outdated copy of virtual partition data.

For example: when a virtual partition boots from its ALT device path and has a config change, and then the virtual partition's nPartition reboots and loads `/stand/vpmon` from the same virtual partition's PRI device path, then as a result the latest virtual partition config changes are not used (but they still reside on the virtual partition's ALT device). Instead, in this example, the `/stand/vpdb` vPars database on the virtual partition's PRI device is used for configuring the nPartition's virtual partitions.

5334

Virtual Partition Console and Log Use on nPartition Servers

On HP nPartition-capable servers, each nPartition has its own console and its own console log that stores a record of recent console activity.

When an nPartition has one or more virtual partitions booted, the nPartition console serves as the console for all virtual partitions loaded/booted in the nPartition.

NOTE

To switch among virtual partition console interfaces, type **Control-a** when accessing the corresponding nPartition console.

In the following example, the user of the nPartition console repeatedly types **Control-a** to cycle through the available virtual partition consoles.

```
feshd3a / Shad [HP Release B.11.11] (see /etc/issue)
Console Login:
Control-a
[Mesh]
Control-a
[Abed]
Control-a
[Danl]
Control-a
[Shad]
Control-a
[Mesh]
```

The above example starts with console access to the virtual partition named "Shad", then switches to the "Mesh" virtual partition console, "Abed" console, "Danl" console, and then back to the "Shad" and finally the "Mesh" virtual partition console.

The service processor (GSP or MP) console log stores nPartition console output, including BCH output and HP-UX `/dev/console` for nPartitions.On nPartition server running virtual partitions, all virtual partitions in the nPartition emit their `/dev/console` output to the nPartition console. Thus, when HP-UX B.11.11 is running in multiple virtual partitions in an nPartition, the nPartition console will display `/dev/console` output for more than one instance of HP-UX.

The nPartition console log also records vPars monitor (vpmon, MON> prompt) output for its nPartition, because the vPars monitor interface is accessed and displayed through the virtual partition's nPartition console.The vpmon event logs file—which is viewable from the `vparstatus -e` command or the vPars monitor's `log` command—only records virtual partition events. It does not record any nPartition chassis codes.The server chassis logs—which are viewable from the service processor (GSP or MP) Show Chassis Log menu—record nPartition and server complex hardware events. nPartition chassis logs do not record virtual partition configuration or virtual partition-specific load/boot events.However, as in non-vPars nPartition environments, the chassis logs do record HP-UX "heartbeat" events and related timeout counter details.

The vPars monitor prompt (MON>) is shared by all virtual partitions in the same nPartition and gives access to commands for loading/booting virtual partitions, displaying virtual partition and system info, reviewing event log history, and performing other tasks.

If multiple nPartitions in a server are running virtual partitions, each nPartition has its own vPars monitor, just as each nPartition runs its own instance of Boot Console Handler (BCH).

S332

Planning Virtual Partition Configurations for HP nPartition Servers

You can use this section to help plan the virtual partition configurations you will establish in nPartitions.

This section covers the following topics:

- *Virtual Partition Hardware Paths* on page 468
- *Listing Available nPartition Hardware Resources* on page 469
- *Virtual Partition Configuration Planning* on page 470

Also see the book *Installing and Managing HP-UX Virtual Partitions (vPars)* for other virtual partition planning info.

S33

Virtual Partition Hardware Paths

You may need to reference the following hardware path info for HP nPartition-capable servers when planning virtual partition configurations.

Figure 11-2 **HP nPartition Hardware Paths for Virtual Partition Configurations**

Processor (CPU) Hardware Paths

cell/10
cell/11
cell/12
cell/13

For all nPartition hardware paths, *cell* is the global cell number (0–15).

HP Superdome — PCI Card Slot Hardware Paths

Slot	11	10	9	8	7	6	5	4	3	2	1	0
Path (LBA)	*cell*/0/8	*cell*/0/9	*cell*/0/10	*cell*/0/11	*cell*/0/12	*cell*/0/14	*cell*/0/6	*cell*/0/4	*cell*/0/3	*cell*/0/2	*cell*/0/1	*cell*/0/0

HP rp7405/rp7410 and HP rp8400 — PCI Card Slot Hardware Paths

Slot	1	2	3	4	5	6	7	8
Path (LBA)	*cell*/0/8	*cell*/0/10	*cell*/0/12	*cell*/0/14	*cell*/0/6	*cell*/0/4	*cell*/0/2	*cell*/0/1

5330

Listing Available nPartition Hardware Resources

This section presents how you can list all available hardware resources in an nPartition server.

The following are common methods of listing available hardware:

- **`vparstatus -A`** lists the available processor, I/O, and memory resources in the local nPartition. This command lists the hardware that has not yet been assigned to any virtual partition.

  Note that `vparstatus -A` command lists processors and I/O using a form of the hardware path notation where a period (`.`) separates each hardware path field rather than a slash (`/`).

- **`ioscan`** lists the assigned and active hardware in the local nPartition or the current virtual partition.

  When HP-UX is booted in a *non-vPars* environment, `ioscan` lists all all active hardware in the local nPartition.

  When HP-UX is booted in a virtual partition, `ioscan` lists only the I/O devices assigned to the current virtual partition and lists processors on active cells in the local nPartition (but it *does not* list bound processors in other virtual partitions).

  Note that `ioscan` can list some processors that are not assigned to the current virtual partition, including unbound processors assigned to other virtual partitions.

- **`mpsched -s`** lists only the assigned and active processors in the current virtual partition or nPartition.

  Note, however, that `mpsched -s` lists the HP-UX CPU IDs for processors, not their hardware paths.

- **`parstatus -C`** lists the configurations of all cells in an HP nPartition-capable server complex, including the number of processors, amount of memory, I/O chassis connections, current usage status, and nPartition assignment.

Also refer to the chapter *Listing and Managing Server Hardware* on page 305 for details.

5329

Virtual Partition Configuration Planning

Table 11-1 is for planning virtual partition attributes and resource assignments.

For each virtual partition, you **must** specify: a virtual partition name, at least one bound CPU, at least one I/O slot, a PRI boot path, and enough memory to boot HP-UX. The *default virtual partition attributes* establish a dynamic configuration that manually boots the `/stand/vmunix` kernel with no boot options.

The “Host Info” column in Table 11-1 includes configuration details for HP-UX networking (the hostname, IP, gateway, and so on).

Also see *Configuring Virtual Partition Resources and Attributes* on page 445.

5328

Table 11-1 Configuration Planning Table for a Virtual Partition

Virtual Partition Name and Host Info	Attributes (* = Default)	Processor Resources	Input/Output Resources	Memory Resources
Virtual Partition Name: ______________	Configuration: Static *or* Dynamic*	Min: _____	Boot Path (PRI): __/0/__/__/__.__ *Note: also must assign the LBA.*	Size (MBytes): _________ *Note:* *1024 MBytes = 1 GByte*
Hostname: ______________	Boot: Manual* *or* Automatic	Max: _____	Altboot (ALT): __/0/__/__/__.__ *Note: also must assign the LBA.*	
IP Address: ___.___.___.___	Kernel Path: /stand/_______ *For example*: /stand/vmunix*	Total: _____	Assigned Slots (LBAs): ___/0/___ ___/0/___ ___/0/___ ___/0/___ ___/0/___ ___/0/___ ___/0/___ ___/0/___	
Gateway: ___.___.___.___ Subnet: ___.___.___.___	Boot Options: __________	Bound CPUs: ___/___ ___/___ ___/___ ___/___ ___/___ ___/___ ___/___ ___/___		
DNS IP: ___.___.___.___ Domain: ______________				

Installing and Configuring vPars on nPartition Servers

This section covers information on installing the vPars software product onto disks that will be used for booting HP-UX on a virtual partition that is loaded in an nPartition.

After a boot disk has both HP-UX and the vPars software product installed, the disk can be booted to be used in either virtual partition or non-vPars environments.

The vPars software install process can occur when you have booted HP-UX from each disk so that HP-UX is running in a non-vPars environment.

You also can install *both* the HP-UX and vPars software simultaneously on a virtual partition when its nPartition is running in vPars mode. To do this issue the `vparboot -p` *`vpname`* `-I...` command from a different virtual partition in the same nPartition to load/boot the virtual partition from an Ignite-UX server. For details see the *vparboot* (1M) manpage or the vPars install documentation listed below.

NOTE The HP vPars software product must be installed on *every boot device* that will be used by virtual partitions. Each virtual partition must have a boot disk where HP-UX B.11.11 and the vPars software product are installed.

NOTE Before installing the HP vPars software product on an nPartition, you must install the Partition Manager B.11.11.01.05 product (or a later Partition Manager release).

For the latest Partition Manager software, see the **`http://software.hp.com`** Web site.

vPars Software Installation for an HP nPartition

This procedure gives a high-level overview of a process for manually installing HP's virtual partitions software product on an nPartition's disks.

The book *Read Before Installing HP-UX Virtual Partitions* has important information you should read before performing this procedure. Also refer to the book *Installing and Managing HP-UX Virtual Partitions (vPars)*.

Step 1. Boot HP-UX on the nPartition using the boot device that will be the primary (PRI) boot device for one of the nPartition's virtual partitions.

Step 2. Install the HP virtual partitions software product on the booted device.

As part of the vPars software installation, the nPartition is rebooted and a new `/stand/vmunix` HP-UX kernel is built.

Step 3. Create the first virtual partition on the device onto which you have installed the vPars software product.

NOTE Only perform this step for the boot disk from which `/stand/vpmon` will be loaded. Do not perform this step for other boot disks.

Other boot disks are automatically updated with copies of the vPars database as needed.

To complete this step, first boot HP-UX from the device, and then use the `vparcreate` and `vparmodify` commands to create the first virtual partition for the nPartition.

Creating the first virtual partition establishes a vPars database (`/stand/vpdb`) for the nPartition.

You can assign each virtual partition resources that are part of the *local* nPartition. Only hardware that is *assigned* to the local nPartition and is *active* can be used by the virtual partitions within the nPartition.

By default the `vparcreate`, `vparmodify`, and `vparstatus` commands use the `/stand/vpdb` file. Although the vPars monitor is not running as you perform this step, these commands will read and write to `/stand/vpdb` if you do not specify a different vPars database file using the `-D` option.

If you want to create multiple virtual partitions within an nPartition you can do so as part of this step, by issuing a `vparcreate` command for each new virtual partition within the local nPartition.

You also can create any additional virtual partitions later, after you have booted the vPars monitor and loaded/booted HP-UX B.11.11 on the first virtual partition.

Step 4. Issue the **`shutdown -r`** command to reboot HP-UX on the nPartition and return to the nPartition's BCH interface.

As needed, interrupt the autoboot process to interact with the nPartition at the BCH interface.

Step 5. Install the vPars software product on each remaining boot device that is to be used to boot HP-UX on one of the nPartition's virtual partitions.

For each virtual partition boot device, you can boot HP-UX from the device in non-vPars mode and then install the vPars software product on the device.

An alternate install method is to load/boot HP-UX on the first virtual partition, and then simultaneously install HP-UX and vPars software on other virtual partitions by using the the `vparboot -p` *`vpname`* `-I...` command. See the *vparboot* (1M) manpage.

You must install both HP-UX and the vPars software for every virtual partition. For example, if you plan to have three virtual partitions in an nPartition then you need at least three boot devices with HP-UX and vPars software installed.

If you intend to have multiple boot disks for a virtual partition—for example, a PRI device and an ALT device—then you need to install HP-UX and the vPars software product on *both* the PRI and ALT devices for the virtual partition.

5324

Procedures for Managing Virtual Partitions on HP nPartition Servers

This section has procedures for performing typical virtual partitions configuration and management tasks on HP nPartition-capable servers.

The following virtual partitions procedures are covered here:

- *vPars Management: Creating a New Virtual Partition in an nPartition* on page 477
- *vPars Management: Deleting a Virtual Partition from an nPartition* on page 481
- *vPars Management: Modifying Virtual Partition Attributes in nPartition Environments* on page 483
- *vPars Management: Listing Virtual Partition Status from an nPartition* on page 485
- *vPars Management: Booting HP-UX B.11.11 on Virtual Partitions in an nPartition* on page 487
- *vPars Management: Rebooting or Shutting Down Virtual Partitions in an nPartition* on page 495
- *Configuring Virtual Partition Autoboot* on page 498

NOTE

The procedures described here use the HP-UX virtual partitions commands and *not* the graphical Virtual Partition Manager utility.

You can perform all tasks in this section with either the commands or Virtual Partition Manager. For info on the Virtual Partition Manager graphical utility see its online help or see the section *Tools for Managing Virtual Partitions on nPartition Servers* on page 449.

See the section *Installing and Configuring vPars on nPartition Servers* on page 472 for details on installing vPars software on nPartition systems.

Also see the section *Managing nPartitions from a Virtual Partition* on page 506 for issues you should be aware of when you perform nPartition config tasks from a vPars environment.

S323

The book *Installing and Managing HP-UX Virtual Partitions (vPars)* also has detailed virtual partitions management information.

Creating a New Virtual Partition

This section gives details on how to create a new virtual partition.

NOTE Before creating a virtual partition you should already have planned how the local nPartition's resources will be assigned to the virtual partitions running in the local nPartition.

See the section *Planning Virtual Partition Configurations for HP nPartition Servers* on page 467 for info on planning virtual partitions configurations for use in nPartitions.

vPars Management: Creating a New Virtual Partition in an nPartition

This procedure creates a new virtual partition from HP-UX running in a virtual partition on an nPartition.

The book *Installing and Managing HP-UX Virtual Partitions (vPars)* also has detailed virtual partitions information.

Step 1. Login to HP-UX running on one of the virtual partitions within an nPartition.

Step 2. Complete all virtual partition resource planning and confirm that the resources are available for the new virtual partition you intend to create.

See the section *Planning Virtual Partition Configurations for HP nPartition Servers* on page 467 for planning details.

Issue the **vparstatus -A** command to list the processors, memory, and I/O busses that are not yet assigned to any virtual partition.

The vparstatus -A command should list all hardware you plan to assign to the new virtual partition. If any hardware you planned to assign is not available then you must either must revise your plans or unassign or otherwise make the hardware available.

```
# vparstatus -A
[Unbound CPUs (path)]:  0.13
                        1.11
                        1.12
                        1.13
                        2.10
```

S321

```
                        2.11
                        2.12
                        2.13
                        6.10
                        6.11
                        6.12
                        6.13
[Available CPUs]:  12

[Available I/O devices (path)]:  0.0.1
                                 0.0.3
                                 0.0.8
                                 0.0.9
                                 0.0.10
                                 0.0.11
                                 0.0.12
                                 0.0.14
                                 2.0
                                 2.0.0
                                 2.0.1
                                 2.0.2
                                 2.0.3
                                 2.0.4
                                 2.0.6
                                 2.0.8
                                 2.0.9
                                 2.0.10
                                 2.0.11
                                 2.0.12
                                 2.0.14

[Unbound memory (Base  /Range)]:  0x0/64
                (bytes) (MB)      0x8000000/6080
[Available memory (MB)]:  6144
#
```

Step 3. Issue the **vparcreate -p...** command to create the new virtual partition and as needed use **vparmodify -p...** to further configure the new virtual partition.

When using the `vparcreate` command you *must specify* the name for the new virtual partition (`-p` *vpname*).

You also should specify the resources that are to be assigned for exclusive use by the virtual partition, including processor (`-a cpu...`) memory (`-a mem...`) and input/output (`-a io...`) resources.

You also can include other virtual partition attributes and settings (such as the autoboot setting) as part of the vparcreate command that establishes the new virtual partition.

```
# vparcreate -p Mesh -a mem::2048 -a io:2/0/14 -a io:2/0/0 -B manual -S dynamic
-a io:2/0/14/0/0.6:BOOT -a cpu:2/10
#
```

To further modify the virtual partition, issue the vparmodify command after vparcreate has created the new virtual partition.

For other details on creating and configuring virtual partitions see the section *Configuring Virtual Partition Resources and Attributes* on page 445.

Step 4. Issue the **vparstatus** command to list the configuration and boot status for the newly created virtual partition.

For detailed virtual partition information, use the **vparstatus -v -p...** command.

If you need to change any of the new virtual partition's configuration details, use the **vparmodify** command.

```
# vparstatus
[Virtual Partition]
                                                                          Boot
Virtual Partition Name          State Attributes Kernel Path               Opts
=============================== ===== ========== ========================= =====
Shad                            Up    Dyn,Manl   /stand/vmunix
Mesh                            Down  Dyn,Manl   /stand/vmunix

[Virtual Partition Resource Summary]
                                          CPU     Num        Memory (MB)
                                 CPU     Bound/   IO   # Ranges/
Virtual Partition Name          Min/Max  Unbound  devs  Total MB     Total MB
=============================== ======= ========= ==== ====================
Shad                              2/  8    2    2    7    0/    0        2048
Mesh                              1/ 16    1    0    3    0/    0        2048
# vparstatus -v -p Mesh
[Virtual Partition Details]
Name:           Mesh
State:          Down
Attributes:     Dynamic,Manual
Kernel Path:    /stand/vmunix
Boot Opts:

[CPU Details]
Min/Max:   1/16
```

S319

```
Bound by User [Path]:  2.10
Bound by Monitor [Path]:
Unbound [Path]:

[IO Details]
   2.0.14
   2.0.0
   2.0.14.0.0.6  BOOT

[Memory Details]
Specified [Base  /Range]:
          (bytes) (MB)
Total Memory (MB):  2048
#
```

S318

Deleting a Virtual Partition

This section describes the procedure for deleting a virtual partition and related issues you may encounter.

NOTE The virtual partition you delete *must* be in a "Down" state.

You can delete virtual partitions that are defined in the currently active vPars database (vpdb) used by the *local* nPartition.

You also can delete virtual partitions from an alternate vPars database that you specify using the `vparremove` command's `-D` *`database`* option.

You *cannot* modify or delete vPars configuration info from inaccessible vPars databases, such as those on currently unused boot disks. (Currently unused boot disks include: disks assigned to a virtual partition that is not in an "Up" state; or disks not currently booted by a virtual partition such as the ALT boot device for a virtual partition that has booted its PRI device.)

vPars Management: Deleting a Virtual Partition from an nPartition

This procedure deletes a virtual partition's configuration info from the currently active vPars database.

Also see the book *Installing and Managing HP-UX Virtual Partitions (vPars)* for virtual partition management info.

Step 1. Login to HP-UX running on one of the virtual partitions in an nPartition.

Step 2. Issue the **vparstatus** command to list the current boot status and high-level configuration information for all virtual partitions defined in the currently active vPars database (vpdb) used by the local nPartition

```
# vparstatus
[Virtual Partition]
                                                                    Boot
Virtual Partition Name         State Attributes Kernel Path         Opts
============================== ===== ========== =================== =====
Shad                           Up    Dyn,Auto   /stand/vmunix
Mesh                           Down  Dyn,Manl   /stand/vmunix       boot

[Virtual Partition Resource Summary]
                                                  CPU    Num       Memory (MB)
```

S317

```
                                   CPU     Bound/    IO   # Ranges/
Virtual Partition Name           Min/Max  Unbound   devs  Total MB     Total MB
============================== =============== ==== ====================
Shad                               2/  8    2    0     7    0/   0          2048
Mesh                               2/ 12    2    0     3    0/   0             0
#
```

Step 3. Issue the **vparremove -p *vpname*** command to delete the specified virtual partition (*vpname*) and then issue the **vparstatus** command to list the new configuration status.

You can delete only virtual partitions that are in a “Down” state, as reported by the vparstatus command (see the example in the previous step).

See the *vparremove* (1M) manpage for details.

```
# vparremove -p Mesh
Remove virtual partition Mesh? [n]  y
#
# vparstatus
[Virtual Partition]
                                                                          Boot
Virtual Partition Name          State Attributes Kernel Path              Opts
============================== ===== ========== ========================= =====
Shad                            Up    Dyn,Auto   /stand/vmunix

[Virtual Partition Resource Summary]
                                          CPU     Num        Memory (MB)
                                   CPU     Bound/    IO   # Ranges/
Virtual Partition Name           Min/Max  Unbound   devs  Total MB     Total MB
============================== =============== ==== ====================
Shad                               2/  8    2    0     7    0/   0          2048
#
```

5316

Modifying Virtual Partition Configuration Attributes

This section describes how to add or remove resources from a virtual partition, and how to change a virtual partition's attribute settings.

Many virtual partition hardware resource changes require that the virtual partition being modified *is not running* (not in an "Up" state).

vPars Management: Modifying Virtual Partition Attributes in nPartition Environments

This procedure describes how to modify a virtual partition's attributes and resource configuration.

Step 1. Login to HP-UX running on one of the virtual partitions in an nPartition, or login to HP-UX running in non-vPars mode on an nPartition.

You can modify virtual partition attributes from HP-UX running in a virtual partition.

You also can modify vPars database configurations when you have booted HP-UX in non-vPars mode. By default the `vparcreate`, `vparmodify`, and `vparstatus` commands use the `/stand/vpdb` file.

To modify a vPars database other than the `/stand/vpdb` file, use the `-D` option to specify its location.

Step 2. Issue the **vparstatus** command to list the current status of the virtual partition you plan to update.

For detailed info on a virtual partition use the `vparstatus -v -p...` command.

```
# vparstatus
[Virtual Partition]
                                                                           Boot
Virtual Partition Name         State Attributes Kernel Path                Opts
============================== ===== ========== ========================== =====
Shad                           Up    Dyn,Manl   /stand/vmunix
Mesh                           Up    Dyn,Manl   /stand/vmunix              boot

[Virtual Partition Resource Summary]
                                           CPU     Num       Memory (MB)
                                  CPU     Bound/    IO   # Ranges/
Virtual Partition Name          Min/Max  Unbound   devs  Total MB    Total MB
==============================  ================   ====  ====================
```

5315

```
Shad                                     2/  8     2   6      7    0/  0          2048
Mesh                                     2/ 12     2   6      3    0/  0          2048
#
```

Step 3. Issue the **vparmodify -p...** command to modify the specified virtual partition.

See the section *Configuring Virtual Partition Resources and Attributes* on page 445 for descriptions of the virtual partitions configuration options.

Also see the *vparmodify* (1M) manpage for details.

For example, the following commands set the virtual partition named "Mesh" to be configured for autoboot; configure "Shad" to have 4 processors; and configure "Mesh" to have 12 processors:

```
# vparmodify -p Mesh -B auto
# vparmodify -p Shad -m cpu::4
# vparmodify -p Mesh -m cpu::12
```

Step 4. Issue the vparstatus command to list the new status for the virtual partition you modified in the previous step.

You can make further changes to the virtual partition by issuing additional vparmodify commands.

```
# vparstatus
[Virtual Partition]
                                                                                Boot
Virtual Partition Name         State Attributes Kernel Path                     Opts
============================== ===== ========== ========================= =====
Shad                           Up    Dyn,Manl   /stand/vmunix
Mesh                           Up    Dyn,Auto   /stand/vmunix                   boot

[Virtual Partition Resource Summary]
                                          CPU     Num        Memory (MB)
                                 CPU    Bound/    IO    # Ranges/
Virtual Partition Name         Min/Max  Unbound  devs   Total MB     Total MB
============================== ================ ==== ====================
Shad                             2/  8    2   2     7    0/  0          2048
Mesh                             2/ 12    2  10     3    0/  0          2048
#
```

5314

Listing the Status for Virtual Partitions

This section covers methods for listing the status of virtual partitions in an nPartition.

You can list virtual partition status details from HP-UX running on a virtual partition. You also can list vPars database details for nPartitions that are not booted in vPars mode.

In addition to the procedure listed below, you can list limited virtual partition status info from the vPars monitor (the MON> prompt) by using the vparinfo monitor command.

vPars Management: Listing Virtual Partition Status from an nPartition

This procedure lists the boot status and configuration details for virtual partitions that are defined in an nPartition.

Step 1. Login to HP-UX running on any of the virtual partitions in the nPartition.

Step 2. Issue the **vparstatus** command for details about virtual partitions.

You can list the status for all virtual partitions, a specific virtual partition, or the vPars monitor's event log.

- To list a summary that includes the status for all currently defined virtual partitions, issue the **vparstatus** command with no arguments or options.
- To list detailed information about a specific virtual partition, issue the **vparstatus -v -p** ***vpname*** command.
- To display history from the vPars monitor's event log issue the **vparstatus -e** command.

  The vPars monitor event log details are available only when the nPartition is booted in vPars mode.

```
# vparstatus
[Virtual Partition]
                                                                          Boot
Virtual Partition Name          State Attributes Kernel Path              Opts
============================== ===== ========== ========================= =====
Shad                            Up    Dyn,Auto   /stand/vmunix
Mesh                            Down  Dyn,Manl   /stand/vmunix            boot
```

```
[Virtual Partition Resource Summary]
                                                 CPU     Num        Memory (MB)
                                         CPU   Bound/    IO    # Ranges/
Virtual Partition Name                 Min/Max Unbound  devs   Total MB     Total MB
============================== ================ ====  ====================
Shad                                     2/  8    2   0     8    0/   0         2048
Mesh                                     2/ 12    2   2     3    0/   0         2048
#
# vparstatus -e
INFO:CPU0:MON:[17:56:51 5/20/2002 GMT] VPAR Monitor version 0.2 started
INFO:CPU0:MON:Version string: @(#) $Revision: vpmon:    vw: --    selectors: CUP
11.11_BL2001_1101 'cup_vpar_pib3' 'cup_shep_sd_vpars'  Sun May  5 20:22:18 PDT
2002 $
INFO:CPU0:MON:cell num 6 does not contain i/o chassis
INFO:CPU0:MON:cell num 1 does not contain i/o chassis
INFO:CPU0:MON:Partition Shad monarch set to 0/10
INFO:CPU0:MON:Partition Mesh monarch set to 2/10
INFO:CPU0:MON:[17:57:45 5/20/2002 GMT] Shad is active
INFO:CPU0:MON:PDC_STABLE return size = 3f0
INFO:CPU0:MON:[17:58:15 5/20/2002 GMT] Shad is up

#
```

S312

Booting HP-UX on Virtual Partitions

This section provides a procedure for loading and booting HP-UX on a virtual partition that is running in an nPartition.

As part of the virtual partition boot process, you will boot the `/stand/vpmon` vPars monitor from the nPartition BCH interface instead of booting the `/stand/vmunix` HP-UX kernel.

From the vPars monitor (the `MON>` prompt) running on an nPartition, you can load one or more virtual partitions. Each virtual partition then can boot a single instance of the HP-UX kernel.

Before performing this procedure, review the following list for an overview of situations you may encounter when loading and booting virtual partitions on an nPartition server.

- If one or more virtual partitions already has loaded/booted HP-UX on the nPartition, you can load/boot additional virtual partitions from HP-UX running on one of the existing virtual partitions.

  In this situation, you can issue the `vparboot` command to load other virtual partitions; see the *vparboot* (1M) manpage for details.

  However, you can only load virtual partitions that are defined in the currently active vPars configuration database, which typically is the `/stand/vpdb` file on the same boot device where `/stand/vpmon` was booted.

- If HP-UX is booted in non-vPars mode on an nPartition, you must shut down HP-UX on the nPartition and from the nPartition's BCH interface boot the `/stand/vpmon` vPars monitor before loading any virtual partitions.

These above situations also are addressed in the following procedure.

vPars Management: Booting HP-UX B.11.11 on Virtual Partitions in an nPartition

This procedure describes how to boot HP-UX on one or more virtual partitions in a single nPartition.

Also refer to the chapters *An Overview of nPartition Boot and Reset* on page 161 and *Booting and Resetting nPartitions* on page 197 for details on booting nPartitions.

Step 1. Login to the service processor (GSP or MP) for the server where the virtual partitions will be booted.

Step 2. Access the console for the nPartition in which the virtual partitions will boot HP-UX.

From the service processor main menu enter **CO** to access the nPartition console menu, and select the nPartition in which you will boot the virtual partitions.

```
GSP> CO

        Partitions available:

          #    Name
        ---    ----
          0)   feshd4a
          1)   feshd4b
          Q)   Quit

        Please select partition number: 0
```

Step 3. Access HP-UX or the BCH interface for the nPartition, and if needed reboot the instance of HP-UX running on the nPartition.

When accessing the nPartition console, if you can interact with a BCH command prompt such as the following:

```
Main Menu: Enter command or menu >
```

then you can proceed to the next step and *skip the rest of this step*.

If you cannot interact with a BCH menu or HP-UX login prompt or command line, then the nPartition might be booting or might be hanged.

You can use the server's Virtual Front Panel (VFP) to check the nPartition's current boot state. Refer to the chapter *Using Console and Service Processor Interfaces* on page 125 for details.

Otherwise, if HP-UX is running in the nPartition, first check to see whether HP-UX booted in vPars-mode or non-vPars mode.

Enter the **vparstatus -w** command, and determine the current nPartition boot state:

- If `vparstatus` reports `Error: Virtual partition monitor not running` then the nPartition is *not running vPars*.

  Enter `shutdown -r` to reboot the nPartition and as needed interrupt the autoboot process to access the nPartition's BCH interface.

After entering the `shutdown` command and accessing the BCH interface you can *proceed with the next step.*

- If `vparstatus` reports `The current virtual partition is...` then the nPartition is *running one or more virtual partitions.*

NOTE

This note applies only when an nPartition is running one or more virtual partitions.

Because at least one virtual partition already has loaded/booted HP-UX on the nPartition, you should check whether the virtual partition you wish to boot already is loaded, or whether the virtual partition can be loaded without rebooting HP-UX.

From HP-UX running on the virtual partition, enter the `vparstatus` command.

If the virtual partition you wish to load/boot *is not listed* in the `vparstatus` output, you may need to reboot the nPartition and its virtual partitions and you can *proceed with the rest of this step and procedure.*

If the virtual partition you wish to load/boot is listed, then check its boot state. If the virtual partition is "Up" then it *already has loaded / booted* HP-UX. If the virtual partition is "Down" then you can load/boot it using the `vparboot` command (see the *vparboot* (1M) manpage). In either of these two cases you can *skip the rest of this procedure.*

If you are certain that you need to reboot the nPartition and its virtual partitions, proceed with the rest of this step.

To access BCH, shut down HP-UX on all virtual partitions and reset the virtual partition.

See the procedure *Rebooting or Shutting Down Virtual Partitions* on page 494 for complete details on shutting down HP-UX on all virtual partitions and returning to the BCH interface. You must shut down and halt (`shutdown -h`) HP-UX in each virtual partition, and then at the vPars monitor's `MON>` prompt enter the `reboot` command to reset the nPartition. When the nPartition resets all active cells in the

S309

nPartition are reset; after the cells reset you should interrupt the nPartition's autoboot process if needed and then access the BCH interface.

Once you have access to the BCH interface proceed with the next step.

Step 4. From the BCH interface enter the **`BOOT`** ***`device`*** command, where *`device`* is the disk where the desired vPars configuration database (the `/stand/vpdb` file) resides.

When using the `BOOT` command you can specify a boot path variable (for example, `BOOT PRI`) or a hardware path for the boot device (for example, `BOOT 0/0/1/0/1.3`).

In addition to having the vPars database (vpdb), the device must have both HP-UX B.11.11 and the vPars software product installed.

Step 5. Instruct BCH to stop the boot process at the ISL prompt by entering **`y`** at the "Do you wish to stop" prompt.

```
Do you wish to stop at the ISL prompt prior to booting? (y/n)
>> y
```

If the boot device's AUTO is set to boot `/stand/vpmon` then you can instead enter `n` (for "do not stop at ISL") and have the nPartition proceed to boot the vPars monitor automatically.

However, you must direct the ISL/SSL interfaces to load `/stand/vpmon` if the boot device's AUTO file *does not contain* the string `hpux boot /stand/vpmon`.

You can check the AUTO file contents from the ISL prompt by entering the `hpux show autofile` command. By default the AUTO file is set to `hpux`, which loads the `/stand/vmunix` kernel.

See *Configuring Virtual Partition Autoboot* on page 498 for details on configuring a boot device's AUTO file.

Step 6. As necessary, from the ISL interface enter the **`hpux boot /stand/vpmon`** command to boot the vPars monitor (vpmon) on the local nPartition.

```
ISL> hpux boot /stand/vpmon

Boot
: disk(0/0/6/0/0.5.0.0.0.0.0;0)/stand/vpmon
565248 + 156368 + 16872200 start 0x23000
```

S308

```
Welcome to VPMON (type '?' for a list of commands)

MON>
```

If you stopped at the ISL interface, you must perform this step.

You do not need to perform this step if the boot device AUTO file is set to `hpux boot /stand/vpmon` and you did not stop at the ISL prompt in the previous step.

Step 7. At the vPars monitor's MON> prompt, enter the **vparinfo** command to list details about the virtual partitions currently defined in the vPars database (vpdb).

Especially note the list of virtual partitions that the `vparinfo` command displays as the "Names of the partitions in the database".

```
MON> vparinfo

Resources not assigned to any partition
-------------------------------------
0           0xfffffffffc000000       1       0   TYPE=14   SV_MODEL=170
0/0         0xffffff808000000        1       0   TYPE= 7   SV_MODEL= 12
0/0/0       0xffffff804000000        1       0   TYPE=13   SV_MODEL= 10
0/0/1       0xffffff804002000        1       0   TYPE=13   SV_MODEL= 10

....

Names of the partitions in the database:
----------------------------------------

Shad
Mesh

Available Free Memory: 0 MB

Available MEM RANGE: 0x0000000000000000-0x00000000ffffffff (4194304 Kb)
MON>
```

To see detailed information about a particular virtual partition you can use the `vparinfo` *vpname* command, where *vpname* is the virtual partition's name. This detailed information includes the resources assigned to the virtual partition and other details such as the virtual partition boot path(s) and the virtual partition's autoboot setting.

Step 8. From the vPars monitor's MON> prompt, use the **vparload** command load/boot HP-UX on a virtual partition.

S307

You can specify any of the following vparload commands at the vPars monitor MON> prompt:

- To load/boot HP-UX on *all virtual partitions* that are defined in the current vPars configuration database, enter: **vparload -all**
- To load/boot HP-UX on *a single virtual partition*, enter: **vparload -p *vpname***

  where *vpname* is the name of the virtual partition, as reported by the vparinfo command in the previous step.
- To load/boot HP-UX only on *the autoboot-enabled virtual partitions*, enter: **vparload -auto**

  This command loads only the virtual partitions that have the autoboot attribute configured (the boot attribute is set to auto).

The following example shows the virtual partition named “Shad” being loaded from the vPars monitor prompt and booting HP-UX.

```
MON> vparload -p Shad
[MON] Booting Shad...
[MON] Console client set to Shad
[MON] Console server set to Shad

[Shad]

[MON] Shad loaded
gate64: sysvec_vaddr = 0xc0002000 for 2 pages
NOTICE: nfs3_link(): File system was registered at index 3.
NOTICE: autofs_link(): File system was registered at index 6.
NOTICE: cachefs_link(): File system was registered at index 7.

    Host is virtual System Console slave
Logical volume 64, 0x3 configured as ROOT
Logical volume 64, 0x2 configured as SWAP

....

     HP-UX Start-up in progress
     __________________________

     Configure system crash dumps ........................................ OK
     Mount file systems .................................................. OK
     Virtual Partitions Initialization ................................... OK
     Update kernel and loadable modules .................................. N/A
     Initialize loadable modules ......................................... N/A
```

S306

```
Setting hostname ..................................................... OK

....
```

Step 9. Login to HP-UX running in the virtual partition you loaded/booted in the previous steps of this procedure.

Because the *nPartition console is shared by all virtual partitions* within the nPartition, you should login using a method other than the system console login for most virtual partition access purposes.

Use the `telnet` command or another remote login method to access HP-UX running on the virtual partition.

After you login to a virtual partition running on an nPartition, you can list the current virtual partition using `vparstatus -w`, and can list the local nPartition's partition number using the `parstatus -w` command.

```
# vparstatus -w
The current virtual partition is Shad.
# parstatus -w
The local partition number is 0.
#
```

S305

Rebooting or Shutting Down Virtual Partitions

This section describes how to reboot HP-UX in a virtual partition and how to shut down all virtual partitions running in an nPartition.

After shutting down all virtual partitions in an nPartition you can reboot the vPars monitor to reset the nPartition and, after resetting, make the nPartition's BCH interface available.

NOTE

The nPartition *reboot for reconfig* and *ready for reconfig state* involve methods of resetting an nPartition that require additional considerations not covered in this section.

See the section *Managing nPartitions from a Virtual Partition* on page 506 for details and procedures to perform a *reboot for reconfig* or to shut down an nPartition to a *ready for reconfig state* when one or more virtual partitions is running in the nPartition.

When you reboot (`shutdown -r`) HP-UX running in a virtual partition, HP-UX will automatically attempt to reboot on the virtual partition *if* the virtual partition is configured for autoboot *and* none of the other virtual partitions in the same nPartition have initiated a reboot for reconfig or a shutdown to the ready for reconfig state.

You can interrupt the virtual partition autoboot process when accessing the virtual partition's console interface through its nPartition's console.

When you halt (`shutdown -h`) HP-UX running in a virtual partition the virtual partition shuts down to a "Down" state and HP-UX does not reboot. After you have halted a virtual partition you can load/boot HP-UX on the virtual partition using the `vparboot` command from HP-UX running on any of the other virtual partitions in the same nPartition. Also see the procedure *vPars Management: Booting HP-UX B.11.11 on Virtual Partitions in an nPartition* on page 487 for other methods and details.

To shut down *all virtual partitions* in an nPartition, login to each virtual partition through its console and halt HP-UX (`shutdown -h`). Then from the vPars monitor's `MON>` prompt you can enter `reboot` to exit the vPars monitor and reset the nPartition's active cells.

S304

vPars Management: Rebooting or Shutting Down Virtual Partitions in an nPartition

The following procedure is for performing a normal reboot (`shutdown -r`) or a shutdown-and-halt (`shutdown -h`) in a virtual partition that is running in an nPartition.

This procedure also describes how to halt all virtual partitions in an nPartition and return to the nPartition's BCH interface.

Step 1. Login to HP-UX running on the virtual partition that you want to shutdown or reboot.

You can login to the virtual partition remotely by using the `telnet` command or another remote login command, or can login through the virtual partition's console.

If you plan to *shut down all virtual partitions* in the nPartition, you should gain console login access to the virtual partitions.

You also will need virtual partition console access for this procedure if you must interrupt the virtual partition's HP-UX autoboot process.

To access the virtual partition's console, first login to the service processor (GSP or MP) for server where the virtual partition's nPartition resides and then access the nPartition's console. As needed, in the nPartition console type **Control-a** to switch among the virtual partition consoles.

Step 2. Enter the **`vparstatus -w`** command to confirm that you are logged into the virtual partition that you want to shut down.

You also can check the virtual partition's autoboot setting by using the `setboot` or the `vparstatus` command.

```
# vparstatus -w
The current virtual partition is Shad.
# setboot
Primary bootpath : 0/0/6/0/0.5.0
Alternate bootpath : 0/0/6/0/0.6.0

Autoboot is ON (enabled)
Autosearch is ON (enabled)

Note: The interpretation of Autoboot and Autosearch has changed
for
```

5303

```
systems that support hardware partitions. Please refer to the
manpage.
#
```

Step 3. From HP-UX running in the virtual partition you want to shut down, enter the **shutdown** command with the appropriate command-line options.
If shutting down *all virtual partitions* in the nPartition, use **shutdown -h**.

To shut down and halt HP-UX on the virtual partition, enter the **shutdown -h** command along with any additional command-line options you need.

To shut down HP-UX on the virtual partition and allow the virtual partition to autoboot HP-UX if it is configured to do so, enter the **shutdown -r** command along with any additional options you need.

See the *shutdown* (1M) manpage for complete details about all options.

Step 4. If you are shutting down *all virtual partitions* in the nPartition, type **Control-a** to switch to the next virtual partition's console login prompt, login to the virtual partition, and then repeat *Step 2* and *Step 3* to shut down HP-UX in the virtual partition.

Typing **Control-a** switches among the virtual partition consoles that are available through an nPartition's console, when one or more virtual partitions are loaded/booted in the nPartition.

NOTE When you type **Control-a** repeatedly in the nPartition console and remain at the vPars monitor (`MON>` or `[MON]`), then no virtual partitions are loaded or booted in the nPartition.

Step 5. If you are shutting down *all virtual partitions* in the nPartition, then after you have halted HP-UX running in each virtual partition in the nPartition you can reset the nPartition by entering the **reboot** command from the `MON>` prompt.

The vPars monitor `reboot` command resets all active cells in the nPartition.

S302

After the cells have reset and completed self-tests, the cells participate in partition rendezvous, form an nPartition, and finally the nPartition's BCH interface is made available through the nPartition console.

If the nPartition is configured to autoboot, you can interrupt the autoboot process by typing any key at the appropriate time when accessing the nPartition's console.

If autoboot is configured for an nPartition, you will see a message similar to the following in the nPartition's console during the nPartition reset process.

```
Attempting to boot using the primary path.
-------------------------------------------------------------

 To discontinue, press any key within 10 seconds.
```

530

Configuring Virtual Partition Autoboot

This section describes how you can configure an nPartition to automatically boot the virtual partitions Monitor and to also boot all virtual partitions that have autoboot configured.

For details on automatically booting HP-UX in *non-vPars mode* on an nPartition, refer to the chapter *Booting and Resetting nPartitions* on page 197.

As the following procedure describes, setting up the virtual partitions autoboot process involves first configuring the nPartition's boot device paths and path flags to boot the device where the current vPars database resides, then configuring that boot device's AUTO file to specify that the vPars monitor be loaded with the `-a` option, and finally configuring the virtual partitions that you want load automatically to have their boot attribute set to auto.

vPars Management: Configuring Virtual Partition Boot Settings

This procedure configures an nPartition to autoboot the vPars monitor (`MON>` prompt) and also automatically load/boot the virtual partitions that have autoboot configured.

Step 1. From the nPartition's BCH interface, configure the nPartition to automatically boot the device where the current vPars database and vPars monitor resides.

First configure one of the nPartition's boot path variables (PRI, HAA, or ALT) to reference the device where the current vPars database (`/stand/vpdb`) resides.

Then configure the nPartition's path flags to boot the chosen device path.

Refer to the chapter *Booting and Resetting nPartitions* on page 197 for details on nPartition autoboot, including device path and path flag configuration.

Step 2. Boot HP-UX in *non-vPars mode* from the device you configured in the previous step.

From the BCH interface, issue the BOOT command and specify the boot path variable you set in the previous step. For example: `BOOT HAA` to boot the HAA device path.

Step 3. Login to HP-UX and configure the chosen boot device's AUTO file.

S300

After HP-UX has booted in non-vPars mode on the nPartition, login as root, use the lvdisplay command to list device file for the boot device, and then use the mkboot command to configure the boot device's AUTO file. You also can use the lifcp command to display the contents of the AUTO file.

For example, the following mkboot command sets the AUTO file for the /dev/dsk/c1t5d0 device, and the lifcp command displays the contents of the device's AUTO file.

```
# mkboot -a "hpux boot /stand/vpmon -a" /dev/dsk/c1t5d0
# lifcp /dev/dsk/c1t5d0:AUTO -
hpux boot /stand/vpmon -a
#
```

The vpmon -a option specifies to automatically load/boot all virtual partitions that have autoboot configured when the vPars monitor is loaded.

Also see the example *Autoboot Configuration Example for Virtual Partitions (vPars)* on page 500 for more example.

Step 4. From HP-UX check all virtual partition boot attributes and reconfigure any boot attributes to establish the virtual partitions autoboot configuration you desire.

Use the vparstatus command to list details about all virtual partitions, including boot attributes. Note that when you issue this command when HP-UX is booted in non-vPars mode, the command presents configuration info based on the /stand/vpdb vPars database.

Then as needed use the vparmodify command to reconfigure any boot attributes. For example, the following command sets the virtual partition named "Mesh" to automatically load/boot HP-UX when possible.

```
# vparmodify -p Mesh -B auto
```

Each virtual partition that you want to boot automatically must have its boot attribute set to auto.

Step 5. Reboot the nPartition, and as desired observe its boot progress from the nPartition's Virtual Front Panel or its console.

The result of this nPartition reboot is to automatically load/boot the virtual partitions that you have configured for autoboot.

5299

Issue the **shutdown -r** command to shut down HP-UX and reboot the nPartition.

When the nPartition reboots to its BCH interface, it will proceed to boot the device path you specified using nPartition boot paths and path flags. The nPartition then will execute the device's AUTO file contents that you specified, to load the /stand/vpmon vPars monitor. Finally, because the vPars monitor is invoked with the -a option, it will automatically load/boot all virtual partitions that have autoboot configured.

Example 11-1 **Autoboot Configuration Example for Virtual Partitions (vPars)**

In this example, the user first confirms that the vPars database (/stand/vpdb) and vPars monitor (/stand/vpmon) are in the /stand directory and thus can be referenced and booted.

The bdf command displays the logical volume associated with the /stand directory, and the the lvdisplay command then displays the device file associated with the logical volume.

```
# ls /stand/vp*
/stand/vpdb    /stand/vpmon
# bdf /stand
Filesystem          kbytes    used   avail %used Mounted on
/dev/vg00/lvol1     512499   71581  389668   16% /stand
# lvdisplay -vk /dev/vg00/lvol1 | grep dev
LV Name                      /dev/vg00/lvol1
VG Name                      /dev/vg00
   /dev/dsk/c1t5d0    128        128
#
```

The first lifcp command that follows displays the original contents of the boot device's AUTO file. Originally, this device is configured with the AUTO file default, hpux, which invokes the hpux loader with no options and thus the /stand/vmunix kernel would be booted.

The mkboot command that follows sets the AUTO file contents so that the hpux loader will boot the /stand/vpmon vPars monitor with the -a option. Issuing the lifcp command again shows the new contents of the device's AUTO file.

```
# lifcp /dev/dsk/c1t5d0:AUTO -
hpux
# mkboot -a "hpux boot /stand/vpmon -a" /dev/dsk/c1t5d0
# lifcp /dev/dsk/c1t5d0:AUTO -
hpux boot /stand/vpmon -a
#
```

S298

Next the user issues the vparstatus command to list the current settings for the virtual partitions defined in the /stand/vpdb file. Because the vparstatus command is issued when the local nPartition is booted in non-vPars mode, the command lists info based on the vpdb file rather than the vPars monitor (which is not running).

```
# vparstatus
vparstatus: Warning: Virtual partition monitor not running, Requested resources
shown.
[Virtual Partition]
                                                                          Boot
Virtual Partition Name         State Attributes Kernel Path               Opts
============================== ===== ========== ========================= =====
Shad                           N/A   Dyn,Manl   /stand/vmunix
Mesh                           N/A   Dyn,Manl   /stand/vmunix

[Virtual Partition Resource Summary]
                                           CPU    Num        Memory (MB)
                                  CPU     Bound/   IO   # Ranges/
Virtual Partition Name          Min/Max  Unbound  devs  Total MB    Total MB
==============================  ================  ====  ====================
Shad                              2/  3    2   0     6    0/  0         2048
Mesh                              1/  2    1   1     6    0/  0         1024
#
```

In this example both virtual partitions, named “Shad” and “Mesh”, originally are configured to be booted manually, as shown in the previous vparstatus command output: the boot attribute for each is listed as “Manl” (manual).

Next the vparmodify command reconfigures the boot attribute for the virtual partition named “Mesh” to auto.

After changing the boot attribute, issuing the vparstatus command shows updated info about “Mesh” and lists its boot attribute as “Auto” (auto).

```
# vparmodify -p Mesh -B auto
# vparstatus -p Mesh
vparstatus: Warning: Virtual partition monitor not running, Requested resources
shown.
[Virtual Partition]
                                                                          Boot
Virtual Partition Name         State Attributes Kernel Path               Opts
============================== ===== ========== ========================= =====
Mesh                           N/A   Dyn,Auto   /stand/vmunix

[Virtual Partition Resource Summary]
                                           CPU    Num        Memory (MB)
                                  CPU     Bound/   IO   # Ranges/
```

```
Virtual Partition Name         Min/Max  Unbound  devs  Total MB    Total MB
============================  ========  =======  ====  =================
Mesh                             1/  2     1   1      6   0/  0        1024
#
```

This example nPartition now is configured so that when the nPartition reboots it will automatically boot from a device that will automatically load a vPars monitor, which then will automatically load/boot the virtual partition named “Mesh”.

In this example’s next step the user reboots the nPartition by issuing the `shutdown -r` command.

```
# shutdown -r

SHUTDOWN PROGRAM
06/26/02 17:57:23 CDT
Waiting a grace period of 60 seconds for users to logout.
Do not turn off the power or press reset during this time.


Broadcast Message from root (console) Wed Jun 26 17:58:23...
SYSTEM BEING BROUGHT DOWN NOW ! ! !

Do you want to continue? (You must respond with 'y' or 'n'.):   y

/sbin/auto_parms: DHCP access is disabled (see /etc/auto_parms.log)


     System shutdown in progress
     ___________________________

     Stopping OpC agent processes (opcagt). .................... OK
     Stop CDE login server ..................................... OK
```

Because the nPartition is booted in non-vPars mode, the `shutdown -r` command shuts down HP-UX and resets the nPartition’s active cells.

After the cells boot and the nPartition reaches its BCH interface, the autoboot process begins.

The following example output shows that the nPartition automatically boots the primary (PRI) boot device path, whose AUTO file is configured to load the vPars monitor and automatically load/boot the virtual partitions whose boot attribute is auto.

The end result of this example nPartition shutdown-and-reboot is that the nPartition has loaded/booted the virtual partition named “Mesh”.

```
Firmware Version  35.3

Duplex Console IO Dependent Code (IODC) revision 1
  ----------------------------------------------------------------------------
      (c) Copyright 1995-2002, Hewlett-Packard Company, All rights reserved
  ----------------------------------------------------------------------------

....

     Primary Boot Path:  0/0/1/0/1.5
          Boot Actions:  Boot from this path.
                         If unsuccessful, go to BCH.

HA Alternate Boot Path:  0/0/1/0/1.6
          Boot Actions:  Go to BCH.


   Alternate Boot Path:  0/0/1/0/1.4
          Boot Actions:  Go to BCH.

          Console Path:  0/0/0/0/0.0


Attempting to boot using the primary path.
-------------------------------------------------------------


 To discontinue, press any key within 10 seconds.

 10 seconds expired.
 Proceeding...

Initializing boot Device.

Boot IO Dependent Code (IODC) Revision 0

Boot Path Initialized.

HARD Booted.

ISL Revision A.00.43  Apr 12, 2000

ISL booting  hpux boot /stand/vpmon -a

Boot
: disk(0/0/1/0/1.5.0.0.0.0.0;0)/stand/vpmon
585728 + 164600 + 16896360 start 0x23000
[MON] Booting Mesh...
MON> [MON] Console client set to Mesh

[MON] Mesh loaded
```

S295

```
    HP-UX Start-up in progress
    __________________________

    Configure system crash dumps ...................................... OK
    VxVM device node check ............................................ OK

....

    Start CDE login server ............................................ OK

The system is ready.

2/0/1/0/0.5 feshd4b (Mesh)  [HP Release B.11.11]
Console Login:
```

In this example, the nPartition has completed the reboot and autoboot process and has automatically loaded/booted the virtual partition named “Mesh”, which has its boot attribute set to auto.

As the following output shows, when the user logs in to HP-UX running on the virtual partition, the vparstatus and parstatus commands report that the *current virtual partition* is “Mesh”, the *local nPartition* is partition number 0, and the virtual partition named “Shad” is in a “Down” state. Shad was not automatically loaded/booted because its boot attribute is set to manual (listed as “Manl” in the output below).

```
Console Login: root
Password:

# vparstatus -w
The current virtual partition is Mesh.
# parstatus -w
The local partition number is 0.
# vparstatus
[Virtual Partition]
                                                                     Boot
Virtual Partition Name         State Attributes Kernel Path          Opts
============================== ===== ========== ==================== =====
Shad                           Down  Dyn,Manl   /stand/vmunix
Mesh                           Up    Dyn,Auto   /stand/vmunix

[Virtual Partition Resource Summary]
                                           CPU      Num      Memory (MB)
                                 CPU      Bound/    IO   # Ranges/
Virtual Partition Name         Min/Max   Unbound   devs  Total MB    Total MB
============================== ================ ==== ====================
Shad                                    2/  3    2   0     6   0/  0          2048
Mesh                                    1/  2    1   1     6   0/  0          1024
#
```

5293

Managing nPartitions from a Virtual Partition

This section covers the nPartition management issues that are unique to virtual partition environments.

NOTE

In virtual partition environments, you can apply the same nPartition configuration tools and principles that you use in non-vPars environments—but you *must take additional steps* to perform a reboot for reconfig of an nPartition that has more than one virtual partition loaded/booted.

The procedures in this section address the minor differences in performing nPartition reconfiguration and reboot for reconfig processes when using virtual partitions in an nPartition.

The following procedures are covered in this section:

- *vPars Management: Determining if an nPartition is Running vPars* on page 507
- *vPars Management: Performing a Reboot for Reconfig or Shutdown to Ready for Reconfig from a Virtual Partition* on page 510
- *vPars Management of nPartitions: Adding and Removing nPartition Cells from a Virtual Partition* on page 513
- *vPars Management of nPartitions: Reconfiguring nPartition Attributes from a Virtual Partition* on page 518

Also refer to the chapter *Managing nPartitions* on page 243 for complete nPartition management procedures.

Virtual partition configuration procedures are covered in the section *Procedures for Managing Virtual Partitions on HP nPartition Servers* on page 475.

5292

Determining if an nPartition is Running vPars

This section gives you several methods for determining if an nPartition has loaded/booted HP-UX in or more virtual partitions. For example, typing **Control-a** at the nPartition console, or using the `vparstatus` command.

vPars Management: Determining if an nPartition is Running vPars

Step 1. Login to the service processor (GSP or MP) for the server where the nPartition resides, and access the nPartition's console. From the main menu, enter `CO` for the console menu and select the nPartition's console.

Step 2. At the nPartition's console, determine the current boot state.

The nPartition's current console prompt, if any, provides the first clue about the boot state:

- If you can interact with a BCH command prompt such as the following:

  ```
  Main Menu: Enter command or menu >
  ```

  Then the nPartition has not booted HP-UX or any virtual partitions.

- If you can interact with a vPars monitor prompt (`MON>`) then the nPartition has *at least* booted the `/stand/vpmon` vPars monitor.

  It is possible that one or more virtual partitions also are loaded/booted.

- If you can interact with the HP-UX console login prompt or the HP-UX command line then you still need to determine if HP-UX has booted in a vPars or in non-vPars mode.

If the nPartition console does not have any interactive prompt or command line, then you can use the Virtual Front Panel to help determine if the nPartition is in the process of booting/resetting or if HP-UX has hanged.

Step 3. When the nPartition's console gives access to the vPars monitor or HP-UX, use additional techniques to determine how many (if any) virtual partitions are loaded/booted.

5291

You can type **Control-a** to switch among the virtual partition consoles. Each time you type **Control-a** the name of the current virtual partition or monitor ([MON]) is displayed in the console window.

If HP-UX is running, login as root and issue the **vparstatus -w** command to list the current virtual partition's name. The **vparstatus** command with no options lists all virtual partitions.

Example 11-2 Checking if Virtual Partitions are Running on an nPartition

The following examples show different nPartition boot states on systems that have the HP vPars software installed.

In the following example, the vPars monitor has booted on the nPartition but virtual partitions have not yet been loaded or booted. Typing **Control-a** repeatedly did not switch to any virtual partitions—only the monitor ([MON]) is running.

```
MON>
Control-a
 [MON]
Control-a
 [MON]
Return
MON>
```

In the following example, HP-UX is running on the nPartition. Although the vPars software is installed, the nPartition is running in non-vPars mode. The vPars monitor is not running, indicating that /stand/vmunix was booted from BCH, not the /stand/vpmon vPars monitor.

```
# vparstatus
vparstatus: Error: Virtual partition monitor not running.
#
```

Finally, in the following example, HP-UX is running on a virtual partition in the nPartition. The current virtual partition is "Shad" and it is the only loaded/booted virtual partition in the nPartition: the other virtual partition named "Mesh" is in a "Down" state.

```
# vparstatus -w
The current virtual partition is Shad.
# vparstatus
[Virtual Partition]
                                                                   Boot
Virtual Partition Name        State Attributes Kernel Path              Opts
============================== ===== ========== ========================= =====
Shad                          Up    Dyn,Manl   /stand/vmunix
Mesh                          Down  Dyn,Manl   /stand/vmunix              boot
```

5290

```
[Virtual Partition Resource Summary]
                                           CPU    Num        Memory (MB)
                                  CPU     Bound/  IO    # Ranges/
Virtual Partition Name          Min/Max  Unbound  devs  Total MB    Total MB
==============================  ================  ====  ====================
Shad                              2/  8    2   0     8    0/  0         2048
Mesh                              2/ 12    2   2     3    0/  0         2048
#
```

5289

Reboot for Reconfig or Shutdown to *Ready for Reconfig* from a Virtual Partition

This section describes how to perform a *reboot for reconfig* and how to shut down an nPartition to the *ready for reconfig* state on nPartitions that are running HP-UX one or more virtual partitions.

A **reboot for reconfig** resets all cell in the nPartition, performs any nPartition reconfigurations, and reboots the nPartition to its BCH interface and allows the nPartition to autoboot, if it is configured to autoboot.

A shut down to the **ready for reconfig state** resets all cell in the nPartition, performs any nPartition reconfigurations, and then holds all cells at a boot-is-blocked state, which makes the nPartition *inactive*.

Refer to the chapter *Booting and Resetting nPartitions* on page 197 for complete details.

vPars Management: Performing a *Reboot for Reconfig* or Shutdown to *Ready for Reconfig* from a Virtual Partition

This procedure covers how to perform a *reboot for reconfig* of an nPartition that is running virtual partitions.

This procedure also describes how to reset an nPartition to a *ready for reconfig* state, for an nPartition that is running vPars.

Step 1. Login to HP-UX running on any of the nPartition's virtual partitions.

Step 2. Issue the **parstatus -w** command to list the local nPartition's partition number, and confirm that you are logged into the virtual partition on the nPartition you want to reboot.

Step 3. Issue the **vparstatus** command to list details about all virtual partitions currently defined in the local nPartition.

Check the command's output to determine whether a reboot for reconfig or a shutdown to ready for reconfig already has been initiated from one of the virtual partitions in the nPartition.

The following note in the `vparstatus` output is presented when either type of reconfig shutdown has been initiated.

S288

```
Note:  A profile change is pending.  The hard partition must be
rebooted to complete it.
```

If this note is presented, then in all other virtual partitions at an "Up" or "Load" or "Boot" state issue the **shutdown -r** command and *skip the next step*.

Step 4. Issue the **shutdown** command with the options appropriate for the type of reboot you want to perform.

You can perform a reboot for reconfig or reset the nPartition to the ready for reconfig (inactive) state.

Use either of the following lists for details.

To perform the *reboot for reconfig* of the local nPartition:

- First issue the **shutdown -R** command in the *current* virtual partition.
- Then in all other virtual partitions at an "Up" or "Load" or "Boot" state, issue the **shutdown -r** command.

  Any virtual partitions in a "Load" or "Boot" state must be shut down *after* they finish loading/booting HP-UX.

  If the nPartition has only one virtual partition—or if all other virtual partitions are in a "Down" or "Shut" state—you do not need to shut down other virtual partitions.

To reset the nPartition to a *ready for reconfig (inactive)* state:

- First issue the **shutdown -R -H** command in the *current* virtual partition.
- Then in all other virtual partitions at an "Up" or "Load" or "Boot" state, issue the **shutdown -r** command.

  Any virtual partitions in a "Load" or "Boot" state must be shut down *after* they finish loading/booting HP-UX.

  If the nPartition has only one virtual partition—or if all other virtual partitions are in a "Down" or "Shut" state—you do not need to shut down other virtual partitions.

Step 5. Monitor the nPartitions boot state by using its Virtual Front Panel. You can access the VFP from the service processor (GSP or MP) main menu.

Refer to the chapter *An Overview of nPartition Boot and Reset* on page 161 for boot status details.

S287

5286

Adding or Removing nPartition Cells from a Virtual Partition

This section describes how you can add cells and remove cells from an nPartition that is running HP-UX in one or more virtual partitions.

See *vPars Management of nPartitions: Reconfiguring nPartition Attributes from a Virtual Partition* on page 518 for details on reconfiguring other nPartition attributes, such as boot paths or the nPartition name, from a virtual partition.

Complete nPartition configuration procedures are given in the chapter *Managing nPartitions* on page 243.

vPars Management of nPartitions: Adding and Removing nPartition Cells from a Virtual Partition

This procedure covers how to add and remove cells from an nPartition that is running the HP virtual partitions software product.

In this procedure, you make changes to the *local* nPartition from HP-UX running in a virtual partition in the nPartition.

For details on modifying remote nPartitions, or nPartitions not currently running vPars, refer to the chapter *Managing nPartitions* on page 243.

NOTE

After *removing* one or more cells from an nPartition, any virtual partitions defined within the nPartition may need to be reconfigured if they explicitly used processor or I/O resources on the removed cell(s).

The vPars software product automatically adjusts virtual partition configurations as needed to account for any expected hardware that is unavailable; as a result, *the vPars database may automatically be changed* after a cell is made inactive or is removed from its nPartition.

After *adding* one or more cells to an nPartition, to use the resources on the new cell(s) you also must modify the nPartition's virtual partition configurations. For example, for a virtual partition to bind the new cell's processors or use any attached I/O slots you must add the resource to the virtual partition by using the `vparmodify` command or the Virtual Partition Manager utility.

5285

Likewise, after an nPartition's inactive cell is made active you also must modify the nPartition's virtual partition configurations to explicitly use the cell's processor or I/O resources.

The following procedure initiates an nPartition cell assignment change from HP-UX running on one virtual partition (using parmodify or Partition Manager) and then *if required* performs a reboot for reconfig of the nPartition.

Step 1. Login to HP-UX running on one of the virtual partitions in the nPartition you want to reconfigure.

You must login as root to perform this procedure.

Step 2. List the local nPartition's partition number to confirm that you are logged into the nPartition you want to modify.

Issue the **parstatus -w** command or use an equivalent Partition Manager procedure to determine the local partition number.

Step 3. Issue the **vparstatus -w** command to list the current virtual partition's name, and then issue the **vparstatus** command (with no options) to list all virtual partitions defined in the local nPartition.

```
# parstatus -w
The local partition number is 0.
# vparstatus -w
The current virtual partition is Shad.
#
# vparstatus
[Virtual Partition]
                                                                   Boot
Virtual Partition Name         State Attributes Kernel Path         Opts
============================== ===== ========== ========================= =====
Shad                           Up    Dyn,Manl   /stand/vmunix
Mesh                           Down  Dyn,Manl   /stand/vmunix             -iS

[Virtual Partition Resource Summary]
                                          CPU     Num        Memory (MB)
                                 CPU      Bound/   IO    # Ranges/
Virtual Partition Name         Min/Max  Unbound  devs  Total MB     Total MB
============================== ================ ==== ====================
Shad                             2/  8    2   2     7    0/   0         2048
Mesh                             2/  8    2   2     3    0/   0         2048
#
```

5284

After you add or remove a cell from the local nPartition, *if required* you will initiate the nPartition's reboot for reconfig from the *current virtual partition only* and will initiate a normal reboot (`shutdown -r`) from all other "Up" (loaded/booted) virtual partitions in the nPartition.

Step 4. Request that the cell(s) be added or removed from the local nPartition.

Use the `parmodify` command or Partition Manager to initiate the cell addition or removal. For detailed information on adding or removing the cell see the following list:

- You should adhere to HP's nPartition requirements and guidelines when adding or removing cells from an nPartition; refer to the chapter *Planning nPartition Configurations* on page 109.
- For details on adding or removing a cell from an nPartition, refer to the chapter *Managing nPartitions* on page 243.

After you have used the `parmodify` command or Partition Manager to modify the local nPartition's configuration, proceed with the next step.

Step 5. Determine if the local nPartition must be shut down to perform a *reboot for reconfig*.

The cell addition and removal procedures referenced in the previous step describe the situations where a reboot for reconfig of the local nPartition is required.

You **must** perform a reboot for reconfig if you removed an *active* cell or you specified the `-B` option to the `parmodify` command. You also **should** perform a reboot for reconfig if you added a cell with a "y" use-on-next-boot value.

You **do not** need to perform a reboot for reconfig if you removed an inactive cell (and did not specify the `-B` option) or if you added a cell with a "n" use-on-next-boot value (and did not specify the `-B` option).

Step 6. *Only if required* to complete the nPartition configuration change, perform a reboot for reconfig of the local nPartition.

First issue the **vparstatus** command to list the state (such as "Up" or "Down") of all virtual partitions in the local nPartition.

```
# vparstatus
[Virtual Partition]
                                                                    Boot
Virtual Partition Name        State Attributes Kernel Path          Opts
```

5283

```
============================== ===== ========== ========================= =====
Shad                           Up    Dyn,Manl   /stand/vmunix
Mesh                           Load  Dyn,Manl   /stand/vmunix             boot

[Virtual Partition Resource Summary]
                                              CPU     Num        Memory (MB)
                                       CPU   Bound/    IO    # Ranges/
Virtual Partition Name               Min/Max Unbound  devs  Total MB    Total MB
==============================      ================  ====  ====================
Shad                                   2/  8   2    0     7    0/   0         2048
Mesh                                   2/ 12   2    0     3    0/   0         2048
#
```

To perform the reboot for reconfig of the local nPartition:

- First issue the **`shutdown -R`** command in the *current* virtual partition.
- Then in all other virtual partitions that are at an "Up" or "Load" or "Boot" state, issue the **`shutdown -r`** command.

  Any virtual partitions in a "Load" or "Boot" state must be shut down *after* they finish loading/booting HP-UX.

  If the nPartition has only one virtual partition—or if all other virtual partitions are in a "Down" or "Shut" state—you do not need to shut down other virtual partitions.

For details see *vPars Management: Performing a Reboot for Reconfig or Shutdown to Ready for Reconfig from a Virtual Partition* on page 510.

After you issue the above `shutdown` commands, HP-UX on the virtual partitions is shut down and the vPars monitor is automatically rebooted.

Because a reboot for reconfig is a *reset of the nPartition hardware*, any virtual partitions that are configured for autoboot do not do so at this time. Instead, the nPartition boot process takes place—including the configured nPartition autoboot behavior (defined by the nPartition's Path Flag settings).

As the reboot for reconfig occurs, *all cells* assigned to the nPartition will reset, any cell assignment changes for the nPartition will occur, and the cells will proceed to perform their self tests.

After the nPartition's cells complete self tests the partition rendezvous can occur and then the nPartition's BCH interface is initiated. If the nPartition is configured to autoboot, then that will occur; otherwise, the BCH interface is made available through the nPartition console interface.

To load/boot all virtual partitions, you can use the normal virtual partition boot methods. See the section *Booting HP-UX on Virtual Partitions* on page 487 for details.

5281

Reconfiguring nPartition Attributes from a Virtual Partition

This section describes how you can modify nPartition attributes from HP-UX running in a virtual partition in the same server as the nPartition.

For details on changing nPartition cell assignments from a virtual partition, see *vPars Management of nPartitions: Adding and Removing nPartition Cells from a Virtual Partition* on page 513.

NOTE

When one or more virtual partitions is loaded/booted on an nPartition, the `setboot` command *affects the current virtual partition's boot settings* and *does not* affect the local nPartition's boot settings.

In this situation, instead use the `parmodify` command to configure nPartition boot device paths from HP-UX.

nPartition configuration data is stored as part of the server Complex Profile and is separate from virtual partition configuration data, which typically is stored in the `/stand/vpmon` file on disk.

For complete nPartition configuration procedures, refer to the chapter *Managing nPartitions* on page 243. Also refer to the chapter *Booting and Resetting nPartitions* on page 197 for boot-related configuration tasks.

vPars Management of nPartitions: Reconfiguring nPartition Attributes from a Virtual Partition

This section covers the configuration of nPartition attributes other than cell assignments, when performing the nPartition configuration from HP-UX running in a virtual partition.

When performing this procedure you *do not* need to perform any reboots.

Step 1. Login to HP-UX running on any virtual partition within the nPartition whose attributes you wish to reconfigure.

Some changes, such as cell attribute changes, require that you initiate the reconfiguration from the local nPartition to which the cell is assigned. When the nPartition is running multiple virtual partitions, you can login to any of the virtual partitions on the local nPartition.

Step 2. Use the **parstatus** command or Partition Manager to list the nPartition's current configuration status.

Step 3. Use the **parmodify** command or Partition Manager to modify the nPartition's configuration. (Do not use the `setboot` command.)

For example, `parmodify -p0 -P NewName` changes nPartition number 0 to be named "NewName".

For other details, refer to the chapter *Managing nPartitions* on page 243.

5279

5276

Index

5277

5276

5275
[redacted]

5274

5273

5072

5271

5270

5269

5268

5267

5266

DOC.
000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE
EQUIPAMENTOS
DE INFORMÁTICA
INCLUINDO
ASSISTÊNCIA
TÉCNICA E
TREINAMENTO

HP INVENT –
MANUAL
APÊNDICES EA A
EZ

2003
PASTA 10

Apêndice EA

Ignite-UX Administration Guide

HP Computers
with HP-UX 10.x, 11.0 or 11i

Manufacturing Part Number : B2355-90772

Edition 10, March 2003
Printed in U.S.A.

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this document and any supporting software media supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Copyright Notice

Trademark Notices

Itanium® is a registered trademarks of Intel® Corporation.

MS-DOS® and Microsoft® are U.S. registered trademarks of Microsoft Corporation.

Netscape ® is a registered trademark of Netscape Communications Corporation.

OSF/Motif™ is a trademark of the Open Software Foundation, Inc. in the U.S. and other countries.

SunForum® is a registered trademark of Sun Microsystems, Inc. in the United States and other countries.

UNIX® is a registered trademark in the United States and other countries, licensed exclusively through The Open Group.

VERITAS® is a registered trademark of VERITAS Software Corporation.

VERITAS File System™ is a trademark of VERITAS Software Corporation.

X Window System™ is a trademark of the Massachusetts Institute of Technology.

Publication History

The manual's publication date and part number indicate its current edition. The publication date changes when a new edition is released. The manual part number changes when extensive changes are made.

To ensure that you receive the new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

- March 1999, Edition 1, HP part number **B2355-90677**.
- December 2000, Edition 2. HP part number **B2355-90704**.
- June 2001, Edition 3. HP part number **B2355-90738**.
- March 2002, Edition 4. HP part number **B2355-90749**.
- June 2002, Edition 5. HP part number **B2355-90750**.
- September 2002, Edition 6. HP part number **B2355-90758**.
- September 2002, Edition 7. HP part number **B2355-90765**.
- October 2002, Edition 8, HP part number **B2355-90770**.
- December 2002, Edition 9, HP part number **B2355-90767.**
- March 2003, Edition 10, HP part number **B2355-90772**.

This guide replaces the *Installing HP-UX 11.0 and Updating from HP-UX 10.x to 11.0* guide, HP part numbers **B23355-90135** and **B2355-90679**.

For the latest version of this and other HP-UX guides, see the HP technical documentation web site at:

`http://docs.hp.com/`

Please direct comments regarding this guide to:

Hewlett-Packard Company
HP-UX Learning Products
3404 East Harmony Road
Fort Collins, Colorado 80528-9599

Or, use this web form to send us feedback:

`http://docs.hp.com/assistance/feedback.html`

Typographic Conventions

We use the following typographical conventions:

audit (5) — An HP-UX manpage. *audit* is the name and *5* is the section in the *HP-UX Reference*. On the web and on the Instant Information CD, it may be a hot link to the manpage itself. From the HP-UX command line, enter “`man audit`” or “`man 5 audit`” to view the manpage. See *man* (1).

Book Title — The title of a book. On the web and on the Instant Information CD, it may be a hot link to the book itself.

Emphasis — Text that is emphasized.

Emphasis — Terms defined for the first time or text that is strongly emphasized.

`ComputerOut` — Text displayed by the computer.

`Command` — A command name or qualified command phrase.

`Computer` — `Computer font` indicates literal items displayed by the computer. For example: `file not found`

`Filename` — Text that shows a filename and/or filepath.

`UserInput` — Commands and other text that you type.

`Variable` — The name of a variable that you may replace in a command or function or information in a display that represents several possible values.

`[ ]` — The contents are optional in formats and command descriptions.

`{ }` — The contents are required in formats and command descriptions. If the contents are a list separated by `|`, you must choose one of the items

`. . .` — The preceding element may be repeated an arbitrary number of times.

`|` — Separates items in a list of choices.

Contents

1. Introducing Ignite-UX

2. Installing and Administering an Ignite-UX Server

3. Using Configuration Files

4. Installing HP-UX with Ignite-UX on Clients Locally

Contents

Contents

B. Using a Boot-Helper System

C. Configuring for a DHCP Server

1 Introducing Ignite-UX

This chapter introduces you to the features and uses of Ignite-UX:

- About this guide.
- Ignite-UX overview.
- Solving problems with Ignite-UX.

About This Guide

This guide describes installing, configuring and using Ignite-UX to facilitate installing and recovering HP-UX on HP computer systems in your computing environment.

This guide is written for experienced HP-UX systems administrators who are responsible for setting up and maintaining HP-UX workstations and servers. They must be familiar with installing HP computer hardware and software, upgrading software, applying patches and troubleshooting system problems. Ignite-UX will help them install new systems and maintain existing ones with less effort than when using individual install and update tools.

Web papers included here

This guide replaces Ignite-UX information in the *Installing HP-UX 11.0 and Updating from HP-UX 10.x to 11.0* guide previously supplied with HP-UX 11.0 media. This guide also includes information from the following papers available on the Ignite-UX web site:

- *Ignite-UX Startup Guide for System Administrators.*
- *Ignite-UX Network System Recovery.*
- *Customized Install Media.*
- *Ignite-UX FAQ*, as of March 2002 (check the web for newer versions).

Documentation and Training

Check the Ignite-UX web site often for announcements, updates to the *Ignite-UX FAQ*, and to download the latest version of Ignite-UX:

`http://software.hp.com/products/IUX`

Details about recent changes to Ignite-UX are in the *Ignite-UX Release Notes* located on the web site or in the directory */opt/ignite/share/doc/release_note*.

Additional information is available on these web pages:

- Ignite-UX and Mirrored disks

  `http://software.hp.com/products/IUX/docs/diskmirror.pdf`

- Ignite-UX System Recovery

  `http://software.hp.com/products/IUX/docs/recovery_merge.html`

- DHCP FAQ

  `http://www.dhcp.org`

Ignite-UX training

HP offers a 3-day classroom course on Ignite-UX for the experienced HP-UX system administrator. For details, classes scheduled in your area, and class registration, go to:

`www.hp.com/education/courses/h1978s.html`

9

Ignite-UX Commands and Online Documentation

Ignite-UX provides online information in the `/opt/ignite/share/doc/` directory. Also see these Ignite-UX manpages:

Table 1-1

Ignite-UX Manpage	Description
ignite (5)	Ignite clients remotely from the Ignite-UX screen and provides an overview of all Ignite-UX commands.
instl_adm (1M) *instl_adm* (4)	Manage Ignite-UX config files.
instl_combine (1M), *make_medialif* (1M)	Construct custom, bootable install media.
instl_dbg (1M)	Debug config files.
instl_bootd (1M)	Boot protocol server for Ignite-UX client.
bootsys (1M)	Reboot and install systems using Ignite-UX.
make_bundles (1M)	Package SD bundles into an SD Depot.
make_depots (1M)	Creates SD depots from media.
make_boot_tape (1M)	Create a system boot tape.
make_net_recovery (4)	Create recovery archives on a network system.
make_tape_recovery (1M)	Create recovery tapes. Replaces `make_recovery` available beginning with Ignite-UX A/B 3.2.
check_recovery (1M)	Check recovery tape status since last `make_*_recovery`.
make_sys_image (1M)	Create golden system images.
make_config (1M)	Generate config files for installing software in SD bundles.

Table 1-1 **(Continued)**

Ignite-UX Manpage	Description
manage_index (1M)	Manage the INDEX file.
setup_server (1M)	Perform Ignite-UX client-server administration tasks.
add_new_client (1M)	Construct and populate a client directory without requiring a reboot.

Ignite-UX Overview

Ignite-UX addresses your need to perform system installations and deployment, often on a large scale. With Ignite-UX, you can:

- Create and reuse standard system configurations.
- Archive a standard system configuration and use that archive to replicate systems.
- Create customized processes to allow interactive and unattended installs.
- More-easily recover your operating system (OS) and applications after crashes and hardware failures.

After running an Ignite-UX install session, you have a working HP-UX client system.

Ignite-UX release versions

Ignite-UX is an HP-UX 10.*x*, 11.0, and 11i product, including 11i v1.6 which supports **Itanium Processor Family** (IPF) systems, that facilitates installing and configuring HP-UX systems. Ignite-UX releases are available to install the HP-UX 10.01, 10.10, 10.20, 11.0 and 11i releases on client systems.

Ignite-UX server software is currently available in these versions:

- HP-UX 10.01, 10.10, 10.20 — version A.3.7.95
- HP-UX 11.0 and 11i— version B.4.0 or later

An Ignite-UX B.*x* server runs on HP-UX 11.0 and 11i and can install HP-UX 10.20, 11.0, and 11i OS and applications on target systems. An Ignite-UX A.*x* server runs on HP-UX 10.*x* and can only install HP-UX 10.*x* software on target systems.

Be sure to check the Ignite-UX web site often for announcements and information on new Ignite-UX releases.

Ignite-UX Features

Client/server control

Ignite-UX install sessions for multiple targets can be controlled from a single server in a true client/server model. A graphical user interface (GUI) called the **Ignite-UX screen** helps you manage multiple, simultaneous install sessions. Alternatively, you can run a single install session from the target system if that is more convenient. A single install server can serve multiple HP-UX releases.

Easy-to-use GUI

The Ignite-UX screen uses tabbed dialogs for task navigation. In addition, a wizard mode is available for the novice.

Multi-sourced installations

You could install your base from one SD depot, a set of patches from another depot, and the applications you want from a third depot all in one session.

Multiple archive formats

In addition to supporting SD software sources, Ignite-UX supports tar, cpio, and pax archives. Tools are provided to help you create a **golden system image** if you wish to install from an archive.

Custom installations

It is easy to create a system that is ready to go as soon as the install session completes. Many of the tasks typically done as separate steps after an install are now incorporated into the Ignite-UX installation process. Ignite-UX allows you to specify what kernel parameters you want set and what user-supplied scripts you would like to run as part of the session. Many different script hooks are provided so you can add your own customizations (during and after the installation). Also, the host and networking information which must normally be supplied at first boot can be specified at install-time. You can:

- Create a configuration for your particular needs, save it, and then quickly apply that configuration to multiple install targets.
- Set up a configuration and then install it on a target machine with no further user interaction. This can be done in both the initial installation and the re-installation cases.
- Scan a system and produce a report detailing what hardware is present, how the disks are used, what kernel modifications have been made, and what software has been loaded. This report can be customized to meet your needs.
- Construct your own customized bootable install/recovery media using the `make_medialif` command.

System recovery

You have consistent, reliable recovery in the event of a catastrophic failure of the system disk or root volume group using either the `make_tape_recovery` or `make net recovery` command.

Support for ServiceControl Manager

Ignite-UX supports installing HP-UX client systems in an HP ServiceControl Manager environment. See the *ServiceControl Manager Installation and Configuration* guide for more details.

Solving Problems with Ignite-UX

Once you have an Ignite-UX server installed and configured for your environment, you'll find that it can help you solve many common installation and recovery problems.

One-step installation

Once you configure a system with a **common configuration** that you want **pushed** to other systems, use Ignite-UX to either manually or automatically Ignite-UX each client system. This common configuration can include any supported HP-UX 10.*x*, 11.0, or 11i OS, plus you can add any required patches and applications. This configuration can be bundled into an OS archive, either on the Ignite-UX server or any system in your environment. You can also **pull** bits from an Ignite-UX server and install the client locally. These processes are explained in Chapters 2 through 5.

Re-install HP-UX or apply patches quickly

You can quickly re-install the OS on an existing system after repair from either an OS archive or SD depots and apply patches. See Chapter 6, Installing Patches with Ignite-UX,and Chapter 7, Using Golden System Images, for details.

Scanning a system

With Ignite-UX, you can easily scan a system, or all systems in your environment, to see what hardware is present, how the disks are used, what kernel modifications have been made and what software has been loaded. See Chapter 5, "Installing HP-UX with Ignite-UX on Clients from a Server," on page 73.

Automate installations

Using Ignite-UX's configuration files allow you to completely automate the OS installation process on any systems in your environment, as explained in Chapter 9, "Automating Installations."

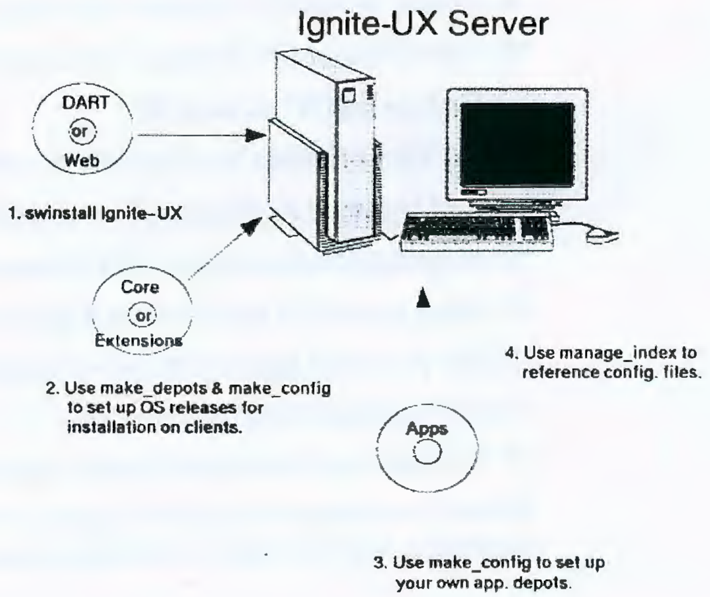
Quick system recovery

In addition to OS archives for initial installations, you can create recovery archives on tape (access from a drive on the client) or on any system in your environment (access via the network). See Chapter 11, System Recovery, for details.

2 Installing and Administering an Ignite-UX Server

This chapter describes installing and configuring an Ignite-UX server.

For on-line information about the Ignite-UX server after it has been installed, see the /opt/ignite/share/doc/ directory and the *ignite* (5) manpage.


Ignite-UX Server
DART
or
Web
1. swinstall Ignite-UX
Core
or
Extensions
2. Use make_depots & make_config to set up OS releases for installation on clients.
Apps
3. Use make_config to set up your own app. depots.
4. Use manage_index to reference config. files.

Installation Overview

Ignite-UX functions as a client-server application. Much of the server configuration will be performed for you in the Ignite-UX installation process, but there are also some separate steps you must take after installation. Tools are supplied to help you complete the server configuration.

Installing Ignite-UX will take care of most server configuration tasks. This can also be done outside Ignite-UX by using either the `setup_server` command as a simple interface or by using the Ignite-UX screen, as explained in this chapter.

Installation tasks

The tasks required to set up an Ignite-UX server are:

"A: Obtain Ignite-UX Software" on page 27

"B: Install Ignite-UX Software" on page 28

"C: Update PATH" on page 29

"D: Set Up or Update the Software Source" on page 29

"E: Add Optional Applications" on page 31

"F: Installing Minimal Ignite-UX Filesets" on page 32

"G: Start Ignite-UX for the First Time" on page 33

"H: Set an Initial Ignite-UX Server Configuration" on page 34

"I: Starting Ignite-UX" on page 36

"J: Configuring Server and Session Options" on page 40

Before proceeding to install an Ignite-UX server, review the server's hardware, software and networking requirements explained next.

Ignite-UX Hardware Requirements

IMPORTANT

NFS Diskless functionality *is not supported* on HP-UX 11.0 and later versions. Do not update your server to HP-UX 11.0 or later versions if you intend to operate that server as a NFS Diskless server.

Server requirements

You will need the following to install an Ignite-UX server:

- **Computer** — A Series 700/800 system running HP-UX 10.0, 10.10, 10.20, 11.0 or 11i. See Ignite-UX version requirements in"Ignite-UX release versions" on page 18.
- **Memory** — Ignite-UX requires 64MB minimum on each server and client. Your HP support engineer can assist in determining the proper amount of RAM.
- **Source Device** — Make sure that your system has an appropriate source (CD-ROM, DVD, DDS drive or LAN card). Ensure that tape drive heads are clean.
- **Disk Drive** — A server needs at least one hard-disk drive with at least the following capacities (`swinstall` performs an analysis of disk space needed prior to loading the software):
  — Generally, 2 GB or more for a usable system, 2.2 GB if on HP-UX 11.0 and 4GB if on HP-UX 11i.
  — Ignite-UX will be loaded under the directory `/opt/ignite`. The data files Ignite-UX creates will be placed under `/var/opt/ignite`. Ignite-UX installation will require approximately 105MB of disk space. You will probably need additional space available under `/var/opt/ignite` for archive and software depot storage.
- **tftp** — Ignite-UX will transfer some of its files using tftp. The minimum directories needed by tftp are set up in the `/etc/inetd.conf` file. Others may need to be added if you place configuration scripts in non-standard locations.
- An additional X11 display server (workstation, X-terminal, PC running an X server, etc). This can be the same system as above.

  - A separate graphics display may be required if a Series 800 Ignite-UX server is being used. Or:
  - The display can be redirected to another X-windows system by setting the DISPLAY environment variable. For example, in the Korn Shell or Posix Shell, enter:

    ```
    export DISPLAY=system_name:0.0
    ```

- Product media or link to the web to load Ignite-UX and any software depots you plan to distribute to target systems.
- Client and server must be on the same subnet if you plan to do the initial boot of the client over the network. A **boot-helper** system can be used to get between subnets and the bootsys command also works between subnets. See Appendix B, "Using a Boot-Helper System," on page 261.

NOTE You can boot over the network only from an Ethernet interface.

Installing an Ignite-UX Server

A: Obtain Ignite-UX Software

Via Media and the Web

Ignite-UX is available from these sources in standard Software Distributor (SD) depot format:

- Application CD-ROM or DVD (if specified when ordering) supplied with HP-UX 10.20, 11.0 and 11i OS media.
- An HP-UX 11i CD1 or DVD (if specified when ordering).
- HP's Software Depot:

  `http://software.hp.com/products/IUX`

  Be sure to obtain the correct Ignite-UX version for your system:

  — For HP-UX 11.0 and 11i, download and install Ignite-UX version B.*x*.

  — For HP-UX 10.20, download and install Ignite-UX version A.*x*.

An Ignite-UX version B.*x* server can install HP-UX 10.20 and 11.0/11i OS and applications on target systems. An Ignite-UX version A.*x* server can only install HP-UX 10.*x* software on target systems.

You may load one or more of the individual `Ignite-UX-1x-xx` bundles onto your system to set up a new Ignite-UX server for installing only that HP-UX version on other systems. That is, you can choose to load a release-specific bundle, such as `Ignite-UX-10-20` for HP-UX 10.20, or an entire bundle such as `B5724AA_APZ`.

IMPORTANT

Do not install individual Ignite-UX server bundles to update an existing Ignite-UX Server. Instead, install the complete bundle for your OS, for example, B5724AA_APZ for HP-UX 10.20. To update yours server to HP-UX 11i, also consider using the new `update-ux` command, as explained in the guide supplied with HP-UX 11i OE media.

Via ftp

You can also access HP's SD Depot via ftp, however this access is "blind"; the `ls` command is not available in the `/ftp` directory. Follow these steps:

Step 1. Log on anonymously to HP's Software Depot:

```
ftp www.software.hp.com
```

Step 2. Move to the `swdepot` directory and get the software bundles you need:

```
ftp> cd /dist/swdepot
ftp> get file_name.tar
```

file_name examples for HP-UX 10.20 servers are:

`ignite_10.01.tar, ignite_10.10.tar, ignite_10.20.tar, ignite_all.tar`

file_name examples for HP-UX 11.0/11i servers are:

`ignite11_10.01.tar, ignite11_10.10.tar, ignite11_10.20.tar, ignite11_11.00.tar, ignite11_ALL.tar`

B: Install Ignite-UX Software

Each software bundle contains the Ignite-UX tools plus the data files required for support of the particular HP-UX release indicated by the bundle name. If you do not wish to load the entire Ignite-UX bundle, see "F: Installing Minimal Ignite-UX Filesets" on page 32.

Step 1. If needed, remove NetInstall. Ignite-UX replaces the capability previously supplied by the NetInstall bundle that came with HP-UX releases 10.01, 10.10 and 10.20. (A system cannot be configured as a server for both NetInstall and Ignite-UX.) Loading any of the Ignite-UX software bundles will give an error until you either remove the NetInstall bundle or touch the `/tmp/okay_to_remove_net_install` file.

Step 2. Once the application CD containing Ignite-UX has been mounted or you have downloaded the Ignite-UX bundle from the web, use `swinstall` to load the desired Ignite-UX bundle(s). You can load the entire product, or you can load only a single Ignite-UX depot if you plan on only using Ignite-UX to install a single release, such as HP-UX 10.20, on client systems. For example, if the Applications CD is mounted at `/cdrom` and you want to load the support for installing HP-UX 10.20 clients onto an HP-UX 10.20 server system, enter:

```
swinstall -s /cdrom Ignite-UX-10-20
```

Or, if you want to install the entire Ignite-UX 11.0 product on an HP-UX 11.0 or 11i server from a software depot on your network located at, say, *hpfclc.fc.hp.com:/release/Ignite-UX*, enter:

```
swinstall -s hpfclc.fc.hp.com:/release/Ignite-UX \
B5725AA_APZ
```

Step 3. After loading Ignite-UX bundle(s), unmount and remove the media and mount the media/drive, if needed, to load the Core software.

C: Update PATH

In your login scripts, add `/opt/ignite/bin` to your default search path:

`export PATH=${PATH}:/opt/ignite/bin` for ksh

or

`set_path = (${path} /opt/ignite/bin` for csh

D: Set Up or Update the Software Source

Ignite-UX allows many options for installing software on target systems. The basic option is to install all software from SD depots on the server. This step describes setting up the software to install on the server.

If you plan to use both SD sources and non-SD sources (tar, cpio, or pax), consider each individually:

For SD OS software

Follow these steps to make an SD source available to Ignite-UX:

Step 1. If you do not already have disk depots, create one using the make_depots command. For example, to create the necessary disk depots that correspond to the HP-UX 10.20 Core CD-ROM or the HP-UX DVD, enter:

```
make_depots -r B.10.20 -s /dev/dsk/c0t0d0
```

This assumes that the CD-ROM or DVD is connected at: /dev/dsk/c0t0d0 and creates one or more depots in the directory: /var/opt/ignite/depots/Rel_B.10.20

Step 2. If you used make_depots as described above to create your depots, use the make_config command to create Ignite-UX config files for each of the depots you plan to use:

```
make_config -r B.10.20
```

This command will create config file for all depots found in the /var/opt/ignite/depots/Rel_B.10.20 directory. It will also add these config files to all INDEX entries for the HP-UX 10.20 release. Skip the next step.

Step 3. If you did not use make_depots to create your depots, run make_config and point it at a specific depot. For example:

```
make_config -s server:/depot_700 \
-c /var/opt/ignite/data/Rel_B.10.20/core_700
```

Now add a reference to the INDEX file:

```
manage_index -a -f /var/opt/ignite/data/Rel_B.10.20/core_700
```

See the *ignite* (5) manpage for further examples.

For non-SD OS software

You will need to create a unique config file that represents the non-SD operating system software. Samples of config files that do a core archive can be found in: /opt/ignite/data/examples/

After copying this file and making edits to it as instructed in the comments contained in the file, you can use the manage_index tool to insert a reference to this configuration in the /var/opt/ignite/INDEX file. Use of configuration files is described in Chapter 3, “Using Configuration Files,” on page 49.

E: Add Optional Applications

If you have other SD-packaged software that you would like to have installed on target clients and want to have the software made available for selection in the Ignite-UX interface, run the make_config and manage_index commands on those depots.

For SD application software

Run the following commands for each depot you plan to load SD software from during the installation. The make_config command only handles SD software which is packaged in bundle form. (All HP-supplied software is packaged in this form. See the *make_bundles* (1M)manpage for information on making SD bundles in an SD depot.)

For example, to make compiler depot bundles available, as root enter:

```
/opt/ignite/bin/make_config\ -s hpfcxxx.hp.com:\
/depots/compiler \
-c /var/opt/ignite/data/Rel_B.10.20/compilers_cfg
```

```
/opt/ignite/bin/manage_index \
-a -f /var/opt/ignite/data/Rel_B.10.20/compilers_cfg
```

Replace the depot server name (in this example: hpfcxxx.hp.com) with the server you have the SD software on. Note that the depot server can be a different system from the Ignite-UX server.

TIP

Rerun the make_config command each time new software is added or modified in the depots.

The make_config command constructs Ignite-UX config files which correspond to SD depots. When an SD depot is used as part of the Ignite-UX process, it must have a config file which describes the contents of the depot to Ignite-UX. This command can automatically construct such a config file, when it is given the name of an SD depot to operate on. This command should be run when adding or changing a depot which will be used by Ignite-UX.

The manage_index command manipulates the /var/opt/ignite/INDEX file. This utility is primarily called by other Ignite-UX tools but can also be called directly.

For non-SD application software

If the source is not an SD depot, the `make_config` command is not applicable. You will need to create a unique config file that references the non-SD software. A sample of a config file that does a non-core archive can be found in: `/opt/ignite/data/examples/noncore.cfg`

NOTE

Do not attempt to use non-core OS archives (such as layered applications) that contain files that get loaded in: `/var/adm/sw/*` Delivering files in this directory in this method may corrupt the SD database.

Step 1. Copy this file to: `/var/opt/ignite/data/Release/configx` Then make the changes to the copy in that directory.

Step 2. After copying and editing this file, use `manage_index` to insert a reference to the copy of the configuration in: `/var/opt/ignite/INDEX`

F: Installing Minimal Ignite-UX Filesets

Depending on what you are using Ignite-UX for, you may be able to reduce the disk space usage by not loading the full product. Below is a list of typical usages and a list of what parts of Ignite-UX you need. If you are not concerned with disk space, just load the bundle(s) for the HP-UX releases you support.

For all cases, the `Ignite-UX.IGNT-ENG-A-MAN` fileset can be omitted or removed if you do not want on-line documentation.

- **Ignite-UX server to install HP-UX on clients**— Load the `Ignite-UX-`*xx-yy* bundle(s) for each HP-UX release (*xx-yy*) which you plan to install onto clients. You can omit the `Ignite-UX.OBAM-RUN` fileset if your server is HP-UX 11i or later and you don't plan on using `make_net_recovery` for HP-UX 10.*x* clients.
- **Ignite-UX server to support network recovery for clients**— You will need the full Ignite-UX-*xx-yy* bundle for each version of HP-UX that your clients are running.
- **Using only make_tape_recovery command:** — You only need these filesets:
  - — `Ignite-UX.RECOVERY`
  - — `Ignite-UX.BOOT-KERNEL`

`Ignite-UX.FILE-SRV-`*`release`* where:

`release` is the HP-UX release of the system you are running

— `Ignite-UX.MGMT-TOOLS`

- **Using only make_net_recovery on a client** —.The filesets a client needs will normally be pushed out by Ignite-UX to each client from the depot created by the `pkg_rec_depot` command. These are the only filesets required for `make_net_recovery` on the client:

  ```
  Ignite-UX.RECOVERY
  Ignite-UX.MGMT-TOOLS
  ```

- **A network boot-helper system** — To setup a system on a remote subnet that is used just to allow a client to do a network boot and then contact a remote Ignite-UX server, all you need is `Ignite-UX.MinimumRuntime`. See “Setting Up the Boot-Helper” on page 262.

G: Start Ignite-UX for the First Time

To start Ignite-UX, as root enter:

```
/opt/ignite/bin/ignite
```

You will get a warning screen stating no clients exists as this is the first time that `ignite` has been invoked. This is normal since you do not have any clients waiting.

If you get this error message:

```
ERROR: This machine is not an NFS server (no nfsd running).
The -n option will not be processed.
```

the Ignite-UX server is not currently on the NFS server. The Ignite-UX server must be an NFS server. Exit Ignite-UX and make the Ignite-UX server an NFS server before continuing. You can do this by using SAM, or by editing `/etc/rc.config.d/nfsconf` to set `NFS_SERVER=1` and rebooting. If you do not get the above error, Ignite-UX has modified your `/etc/exports` file to include the `/var/opt/ignite/clients` directory:

```
exportfs -v
/var/opt/ignite/clients -anon=2
```

This directory is exported to allow remote root users to write to the client's directory. This is required for proper Ignite-UX operations. You may need to export additional directories. For example, if you use NFS to transfer your archive, it must be NFS accessible.

A quick tour

After you have Ignite-UX up and running, you will see the Welcome screen and then the Ignite screen. When you have booted each client you will see an icon representing it on the Ignite-UX screen:

- Click once on a client icon to select it for further actions.
- Double-click the client icon to get a Client Status screen.
- Right-click a client icon to get an Actions menu similar to the pull-down **Actions** menu.

To learn more about the server, step through the quick tutorial. To get started, select:

Actions –> **Run Tutorial/Server Setup** and click **Tutorial and Demo**

For more information on these screens, see Chapter 4, "Installing HP-UX with Ignite-UX on Clients Locally," on page 63.

H: Set an Initial Ignite-UX Server Configuration

Follow these steps to complete the initial server configuration:

Step 1. Select: **Options** –> **Server Configuration**

Step 2. Select the **Server Options** tab.

If needed, modify the Server Options to match the following:

- Default Configuration: (your selection)
- Default Printer: (select a default printer to be used by Ignite-UX)
- Client Timeouts: `40` (the number of minutes delay before the Ignite-UX server will inform the administrator of a network problem or client failure)
- Run client installation UI on: `server` (most administration of the install process to be performed only on the Ignite-UX server)

Step 3. Select: **Add Booting IP Address**

During the install process, the clients need to do a network boot from the Ignite-UX server. In order to do this, the clients need to be given a temporary IP address.

Under **Booting Clients**, enter an initial range of available IP addresses. This example allows Ignite-UX to perform 20 simultaneous installations:

```
15.2.73.1        15.2.73.20
```

This IP address is only used when booting over the network during the initial transfer of the kernel to the client. You may only need one or two addresses depending on how many systems do network boots at the same time. For more information see the *instl_bootd* (1M) manpage. If you need to change these addresses later, you will need to edit: `/etc/opt/ignite/instl_boottab`

Permanent IP addresses are distributed via DHCP Services.

Unless you are familiar with DHCP services, for this exercise, do not modify the "DHCP Class ID" or the "DHCP Addresses Temporary" field. The DHCP service is only used for client configurations which do not have predefined system hostnames and IP addresses.

Provide a range of available "permanent" IP addresses. These can only be supplied once here in Ignite-UX. After the initial definition, use SAM's **Networking and Communications** –> **Bootable Devices** area. For example, we use these IP addresses in our network:

```
15.2.73.21       15.2.73.40
```

Step 4. Select: **Options** –> **Server Configurations** –> **Session Options**

Verify that only these options are set:

```
Confirm new clients
Show the welcome screen for the install server
```

You may wish to de-select **Ask for customer information**, as this installation information is geared to HP and HP distributor-partner manufacturing.

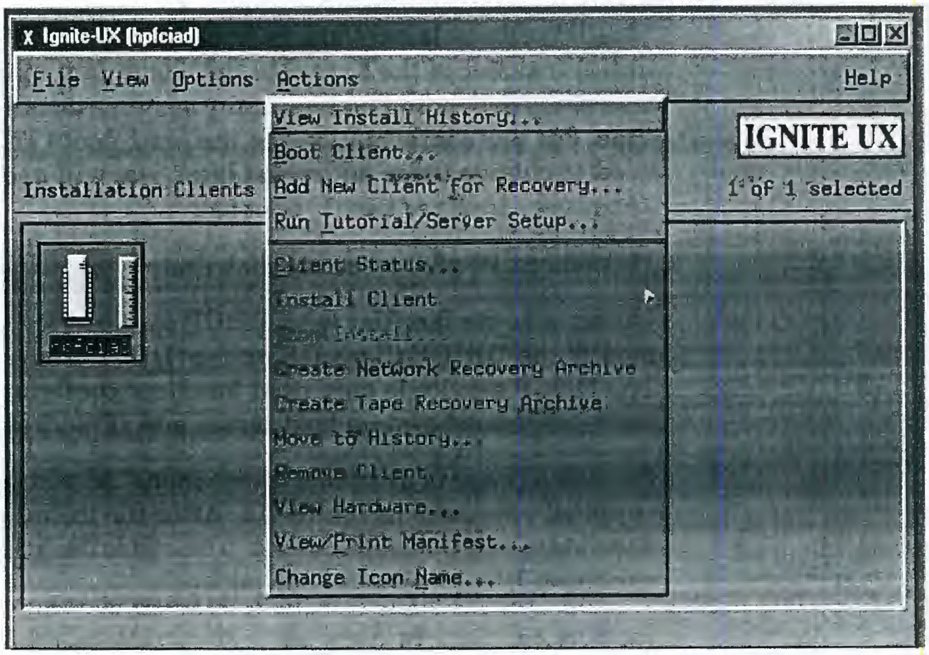
I: Starting Ignite-UX

To start `ignite` on the Ignite-UX server, as root enter:

```
/opt/ignite/bin/ignite
```

Client/server screen

After the Welcome screen is acknowledged by clicking **OK**, Ignite-UX displays its client/server screen as in the following:



Ignite-UX displays each system's installation status via the colored border around each system icon:

- **Green** — OS completely installed, booted and running.
- **Red** — Partially installed or installation stopped. The light blue installation indicator shows the relative progress.
- **No color** — OS not installed.

Client icons represent all booted systems and those systems that can be used for recovery systems. These systems are known to Ignite-UX via `/var/opt/ignite/clients`. If a client is not yet running an OS, see the booting procedure at the end of this chapter. If the client is already running an OS, this can be accomplished remotely by selecting **Actions -> Boot Client**

Actions menu

Select a client (click its icon) and select the **Actions** menu to review available actions for that client:

- **View Install History** — Lists details of all successfully installed clients.
- **Boot Client** — Allows you to boot the selected client.
- **Add New Client for Recovery** — Allows you to identify a client to be recovered.
- **Run Tutorial/Server Setup** — Displays the Welcome screen and you can choose to run the **Tutorial and Demo** or **Server Setup** options.
- **Client Status** — Allows you to see the status of a given client, see "Review client status" on page 39 for more information.
- **Install Client** — Starts the HP-UX installation process for the selected client. This process is explained in Chapter 5, "Installing HP-UX with Ignite-UX on Clients from a Server.".
- **Stop Install**— Stops the install process on the selected client. You can now reboot or halt the client.
- **Create Network Recovery Archive** — Initiates creating a network recovery archive using the `make_tape_recovery` command. See Chapter 11, System Recovery, for more details.
- **Create Tape Recovery Archive** — Initiates creating a recovery archive using the `make_tape_recovery` command. See Chapter 11, System Recovery, for more details.
- **Move to History** — Saves critical files for the client, adds them to the history file and removes the client icon. The client must be "complete" (fully installed) for the configuration to be moved to the history file.
- **Remove Client** — Deletes the icon for the selected client configuration. Client data except for the recovery archive is removed.
- **View Hardware** — Lists hardware associated with the selected client.

- **View/Print Manifest** — Allows you to see or print the manifest and/or Software Certificate. The manifest is also available in saved form on the client and server systems after the installation as the manifest files. On the client, the manifest is in:`/var/opt/ignite/local/`

  On the server, it is in: `/var/opt/ignite/clients/0x`*LLA*`/`

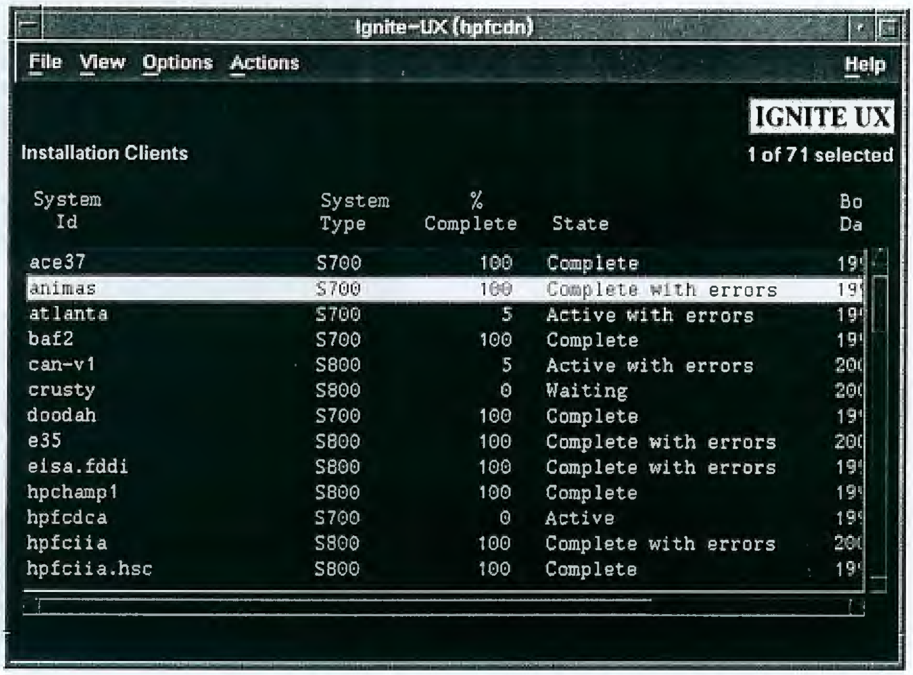
  For an example, see "Viewing and Printing a Manifest" on page 104.
- **Change Icon Name** — Displays a form for renaming the icon for the selected client.

View menu

Use the **View** menu selections to customize the Ignite-UX screen for your needs:

- **Columns**— Re-arrange icons by system attributes.
- **Filter** — View a selected subset of system icons per selected criteria.
- **Sort**— Sort the displayed icons per selected criteria.
- **By Properties** — List clients in a text format rather than with icons. To return to the default icon display, select: **View** –> **By Name and Icon**.

  Using the **By Properties** view along with sorting by **% Complete** can make it easier to quickly scan for clients that have finished installing. Select **Descending Direction** to have all completed systems listed at the top of the display. Here's a portion of a **By Properties** view:



Installation Clients

1 of 71 selected

System Id	System Type	% Complete	State	Bo Da
ace37	S700	100	Complete	19
animas	S700	100	Complete with errors	19
atlanta	S700	5	Active with errors	19
baf2	S700	100	Complete	19
can-v1	S800	5	Active with errors	20
crusty	S800	0	Waiting	20
doodah	S700	100	Complete	19
e35	S800	100	Complete with errors	20
eisa.fddi	S800	100	Complete with errors	19
hpchamp1	S800	100	Complete	19
hpfcdca	S700	0	Active	19
hpfciia	S800	100	Complete with errors	20
hpfciia.hsc	S800	100	Complete	19

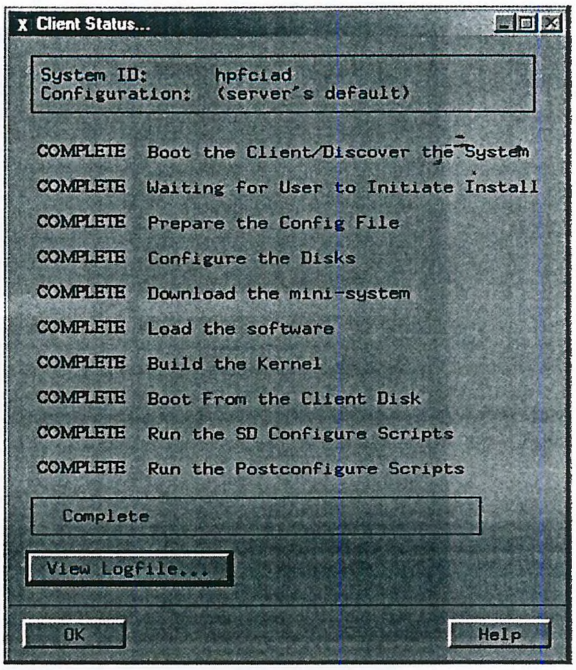
Review client status

After you see client systems displayed on the Ignite-UX screen, you can review the status of any client by:

Step 1. Click once on a client icon to select it for further actions.

Step 2. Double-click the client icon to get the **Client Status** screen, or select Client Status from the Actions menu, or *right-click* a client icon to get a menu similar to the pull-down **Actions** menu.

Any of these actions result in the status of the client being polled and displayed as in the following example:



```
System ID:       hpfciad
Configuration:   (server's default)

COMPLETE   Boot the Client/Discover the System
COMPLETE   Waiting for User to Initiate Install
COMPLETE   Prepare the Config File
COMPLETE   Configure the Disks
COMPLETE   Download the mini-system
COMPLETE   Load the software
COMPLETE   Build the Kernel
COMPLETE   Boot From the Client Disk
COMPLETE   Run the SD Configure Scripts
COMPLETE   Run the Postconfigure Scripts

Complete
```

J: Configuring Server and Session Options

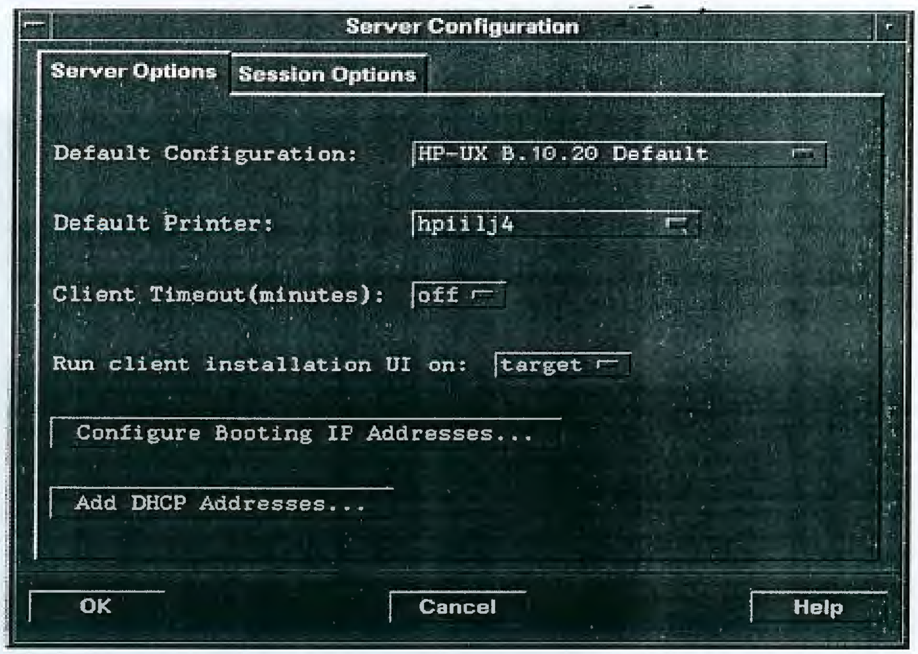
The Ignite-UX server and session options must be configured as described in this section.

Use fields in the **Options** -> **Server Configuration** -> **Server Options** and **Session Options** tabs to:

- Set up your network installation **Precision Architecture Reduced Instruction Set Computing** (PA-RISC or PA)-based or IPF-based server. Network installation details when using Ignite-UX versions B.4.1 and B.4.2 are found in “Release Specific Server Configuration” on page 46.
- Configure the IP addresses to be used for initially booting the install clients (target systems).
- Configure the DHCP address range to be used for directing the client installation process.

Configuring server options

Step 1. Select **Options** –> **Server Configuration**



```
Default Configuration:      HP-UX B.10.20 Default
Default Printer:            hpiilj4
Client Timeout(minutes):    off
Run client installation UI on:  target
```

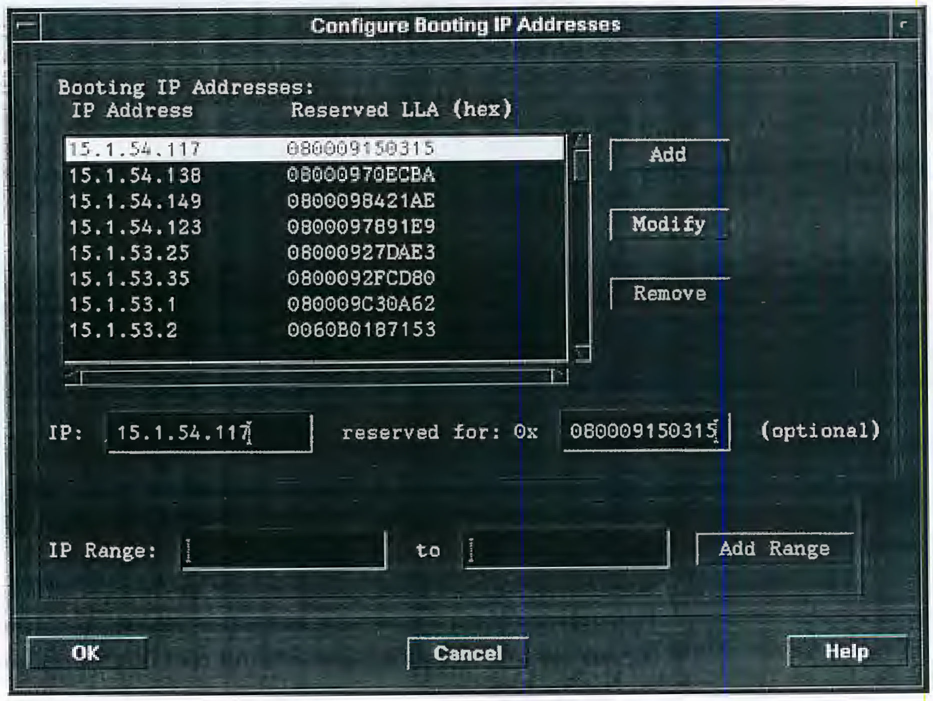
Step 2. Select the **Default Configuration** box and highlight the OS or OE you want. The selected configuration from this list will be installed on to the client's target system. The default setting can be overridden on a per-client basis by Ignite-UX.

Step 3. Click on the **Default Printer** pull-down menu to display the available (configured) printers. Select the one you want to use. If needed, use the **System Administration Manager** (SAM) **Default Printer** area to configure a new printer onto the system. This will be the printer for printing the manifest or installation history. The printer IP address will be checked by Ignite-UX before a job is sent.

Step 4. Select the appropriate **Client Timeout** value, **on** or **off**. This will set a limit on the time since the client install log has been written into. Some points in the installation may require 15 to 30 minutes. A warning note will be displayed if this time is exceeded.

Setting Client Timeout to **off** disables this notification.

Step 5. Use the **Run client installation UI on** menu to designate where you want to view the client UI for this installation. If you have a server configured, you have the choice of running the client installation interface from either the **target** (as a TUI) or **server** (as the Ignite-UX screen). If the client installation is to be non-interactive (no user intervention), select **none**.



Booting IP Addresses:

IP Address	Reserved LLA (hex)
15.1.54.117	080009150315
15.1.54.138	08000970ECBA
15.1.54.149	0800098421AE
15.1.54.123	0800097891E9
15.1.53.25	08000927DAE3
15.1.53.35	0800092FCD80
15.1.53.1	080009C30A62
15.1.53.2	0060B0187153

IP: 15.1.54.117 reserved for: 0x 080009150315 (optional)

IP Range: to

The default location for the GUI to be displayed is the Ignite-UX server.

Step 6. If you are using Ignite-UX version B.4.0 or earlier, you can configure which Ignite-UX servers are used to boot client servers in two ways using the GUI: by identifying IP or DHCP addresses. Select one of the following methods:

a. Click **Configure Booting IP Addresses**
Enter the appropriate IP addresses for the initial boot of the target systems. The number of such addresses determines the number of simultaneous boots you can do.

TIP Be sure that IP addresses entered here are not assigned elsewhere, or you could (re)boot the wrong system.

These IP addresses are used to initially boot ~~target~~ systems. They are used until the system is assigned one of the DHCP boot addresses. One address is required for each simultaneous boot. Typically one to three are needed, depending on your usage.
This data can also be configured by using the `/opt/ignite/lbin/setup_server` command. Or, you can directly edit the `instl_boottab` file; this is necessary for modifying the list order for existing IP addresses.
See the *instl_bootd* (1M) manpage for further details.

Or

b. Click **Add DHCP Addresses** Ensure that the listed IP addresses are not assigned elsewhere. These IP addresses are used during the OS download and application loading. The addresses are in use for most of the Ignite-UX download to a target machine. One address is required for each simultaneous download. You should set more, if the addresses are assigned permanently.

Click the **Temporary** box if you would like to manage a small group of temporary IP addresses, just for use in doing installations, and then reassign the clients new addresses when they are deployed.

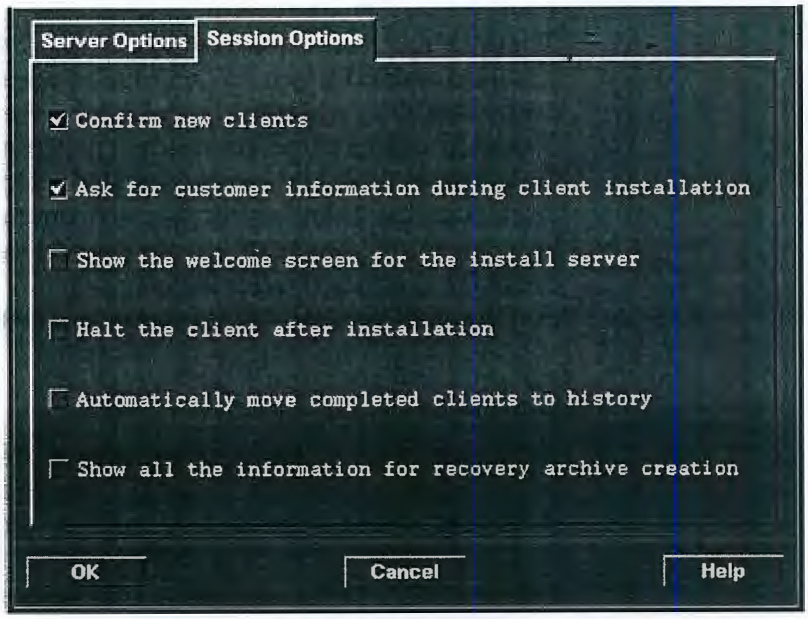
The provision of DHCP capability is for the purpose of installation only and you may want to limit configurations so that they do not interfere with prior DHCP server functions.

See Appendix C, Configuring for a DHCP Server, for details on configuring for DHCP. See the *setup_server* (1M) and *instl_adm* (4) manpages for more information on setting up DHCP functions, addresses and class IDs.

Configuring session options

To configure client response behavior, select:

Options –> Server Configuration –> Session Options



☑ Confirm new clients

☑ Ask for customer information during client installation

□ Show the welcome screen for the install server

□ Halt the client after installation

□ Automatically move completed clients to history

□ Show all the information for recovery archive creation

- **Confirm new clients** — Controls the appearance of a dialog window each time a new client is booted from the Ignite-UX server.
- **Ask for customer information during client installation** — Controls the appearance of an input window for Customer Name, System Serial Number, and Order Number. You may want to refrain from using this option as this information is geared to HP and HP distributor-partner manufacturing.
- **Show the welcome screen for the install server** — If selected, Ignite-UX automatically displays the Welcome screen. This is a useful default if many new operators run Ignite-UX.
- **Halt the client after installation** — Controls whether the client system is halted (rather than the default, reboot) after installation.
- **Automatically move completed clients to history** — Select this button to automatically add completed clients to the end of the history log, `/var/opt/ignite/clients/history/history.log`. It will also move their config and manifest files to the history directory on the

Ignite-UX server for future reference. The client icon will be removed from the client/server screen. The client must be `complete` (fully installed) for this to take place.

- **Show all the information for recovery archive creation.**

Your Ignite-UX server is now ready to ignite HP-UX on client systems in your network.

Proceed to Chapter 4, Installing HP-UX with Ignite-UX on Clients Locally, or to Chapter 5, Installing HP-UX with Ignite-UX on Clients from a Server, depending on where you want to execute the Ignite-UX process.

Release Specific Server Configuration

With the release of Ignite-UX B.4.1, unique server configurations have become necessary. The server specific configurations described in this section are considered cumulative with each release unless specifically stated otherwise.

Follow the specific server configuration that is appropriate for the Ignite-UX version you are installing:

Ignite-UX B.4.2 PA/IPF Server Setup

The Ignite-UX B.4.2 and later releases provide enhanced support for server response to anonymous IPF clients with changes to the `instl_bootd` server. This enhancement is available for both PA and IPF server architectures.

The changes to `instl_bootd` requires that the `bootpd` daemon is not running on the given Ignite-UX server, rather the `instl_bootd` daemon is used by Ignite-UX to respond to all boot requests from clients. The `instl_bootd` daemon normally runs on a set of unique network ports, 1067/1068, that are used only for booting IPF clients. However, in this implementation the `instl_bootd` will run on the standard `bootpd` ports, 67/68.

Using `instl_bootpd` to support anonymous IPF clients

Follow these steps to configure your server to run `instl_bootd` as a replacement for `bootpd`:

Step 1. Set up your Ignite-UX server as described in “Installing an Ignite-UX Server” on page 27.

Step 2. Once your server has been setup, ensure that `bootpd` is disabled on ports 67/68 by commenting out the following line in `/ect/inetd.conf` as shown in this example:

```
#boots dgram udp wait root /usr/lbin/bootpd bootpd
```

Step 3. Restart the `inetd` daemon:

```
/usr/sbin/inetd -c
```

Step 4. Enable the `instl_bootd` daemon on ports 67/68 by adding the following line to `/ect/inetd.conf`:

```
boots dgram udp wait root /opt/ignite/lbin/instl_bootd
instl_bootd
```

Step 5. You must restart `inetd` again to invoke the change made in the previous step:

```
/usr/sbin/inetd -c
```

See the *instl_bootd* (1M) and *inetd* (1M) manpages for more details. Your Ignite-UX server is now configured to respond to anonymous clients.

Ignite-UX B.4.1 IPF Server Setup

Ignite-UX release B.4.1 and later support the installation of IPF systems running HP-UX 11i Version 1.6.

Configuring DHCP support for anonymous IPF clients

Network installation of an IPF system with Ignite-UX B.4.1 requires that you perform the following unique network installation steps.

Step 1. At a minimum, the Ignite-IA-11-22 bundle should be loaded on your system. If it is not, load this bundle with `swinstall`.

Step 2. Add your client's entries to `/etc/bootptab` on the server. The following example is provided in `/etc/bootptab` :

```
ignite-defaults:\
        ht=ethernet:\
        hn:\
        bf=/opt/ignite/boot/nbp.efi:\
        bs=48
System-IPF:\
        tc=ignite-defaults:\
        ha=00d009000000:\
        ip=190.40.101.22:\
        sm=255.255.248.0:\
        gw=190.1.48.1:\
        ds=190.1.48.11
```

All entries in the `ignite-defaults` section can be used without modification.

Duplicate (cut and paste) the `System-IPF` entries and change this section in the following ways:

1. Change `System-IPF` to reflect the client system's hostname.
2. Change the `ha` and `ip` fields for that client.
3. Change the `sm`, `gw`, and `ds` fields to reflect your network.

You can modify the system name, hardware address, IP address and other information for the client.

The following describes fields you may need to change per system and which fields are unique to your network:

- The **ha** field requires setting to the hardware address (`Mac` or *LLA* address of the client system). This address can be found from the firmware's user interface when adding a boot option. See , "IPF Client Network Booting Option" on page 70 of Chapter 4. If the system is up and running, the `lanscan` command can also be used to find this value.
- The **ip** field is the IP address that has been reserved for the client you are about to install and must be an IP address that is valid for your network.
- The **sm** field is the network subnet mask and is probably the same for all systems on your network.
- The **gw** field is the network gateway. It is optional for booting purposes, but useful to provide the system defaults.
- The **ds** field is the domain name server (DNS) and is also optional for booting purposes, but useful to provide as a default.

Step 3. Enable `bootp` services in the `/etc/inetd.conf` file by uncommenting the `bootps` entry.

Step 4. Restart the Internet daemon by entering:

```
/usr/sbin/inetd -c
```

See the *bootpd* (1M) and *inetd* (1M) manpages for more details. Your Ignite-UX server is now configured to respond to anonymous clients.

3 Using Configuration Files

This chapter introduces Ignite-UX configuration files and shows example config-file applications. See Chapter 9, "Automating Installations," on page 135 for more examples of config files.

config Files

Ignite-UX's central data store is called a **config file**. A config file can be thought of as a recipe for how to construct a target system. The config file is expressed in a language designed for this purpose. The language is fully defined in the *instl_adm* (4) manpage. The syntax is human-readable; config files may be created directly by you or via the Ignite-UX screen. The config file language is much like programming languages in that it supports the use of variables and conditional expressions.

Most of the important elements which make up an installed system can be described in the config file:

- Disk and file system layout.
- Software to be installed.
- Target system's identity and network-configuration kernel modifications (additional drivers or tunable parameter settings).
- User-defined scripts which will run at various points in the installation process to further customize the target system.

Types of config Files

For maintenance convenience, the configuration information is split into several types of config files:

- **Default disk and file system layout** — Because the capabilities of each operating system release differ somewhat, HP supplies a different set of defaults for each release. These are located in: `/opt/ignite/data/Rel_`*`release`*`/config`

  where: *`release`* is the result of the `uname -r` command. For example, this file contains the default disk layout for HP-UX 10.20: `/opt/ignite/data/Rel_B.10.20/config`

- **Software description of a single SD depot** — Config files which describe software available from SD depots can be automatically generated via Ignite-UX's `make_config` tool. This tool produces one config file per SD depot. Software description config files are located in: `/var/opt/ignite/data/Rel_`*`release`*`/*`

- **Software description of an archive** — Config files can be hand built to allow access to archives (templates are provided with Ignite-UX in `/opt/ignite/data/examples/` to give you a good starting point). Archives may be in either tar or cpio format. Archive software description config files are also located in: `/var/opt/ignite/data/Rel_`*`release`*`/*`
- **Local configuration overrides that apply globally** — It is often convenient to specify defaults which will be applied to every system installed from a particular server. For example, you might want to specify the same NIS domain for all systems. Place overrides in: `/var/opt/ignite/config.local`
- **Boot control parameters and networking information** — It is possible to specify defaults for attributes like the IP address of the Ignite-UX server and whether to run a UI to install a new target. These can be specified in the first 8KB of the install file system, `/opt/ignite/boot/INSTALLFS` . Use the `instl_adm` command to add, change, or delete this information.
- **Client-specific configuration files** — Each client to be installed has a unique configuration file located at: `/var/opt/ignite/clients/0x`*`LLA`*`/config`

  LLA is the link-level address of the client. This file is typically created when using the Ignite-UX user interface to specify the target system configuration.

  This file usually refers to other config files mentioned above. It also contains specific directives to override what may have been defined in the other files. For example, you may wish to customize the disk layout beyond what the defaults allow in: `/opt/ignite/data/Rel_`*`release`*`/config`

  The customizations appear in: `/var/opt/ignite/clients/0x`*`LLA`*`/config`
- **Named configurations created by saving a configuration via Ignite-UX screen**— You can create your own default configurations via the Ignite-UX screen and save them for future use. For example, you might have a large number of users with similar systems who all run CAD tools. You could build a configuration which matches what they need and save it in a configuration called "CAD System". When you need to install a new system of this type, you can select **CAD**

System from the UI and you're done (or you could customize it further using CAD System as the template). Saved configurations are located in: /var/opt/ignite/saved_cfgs/*

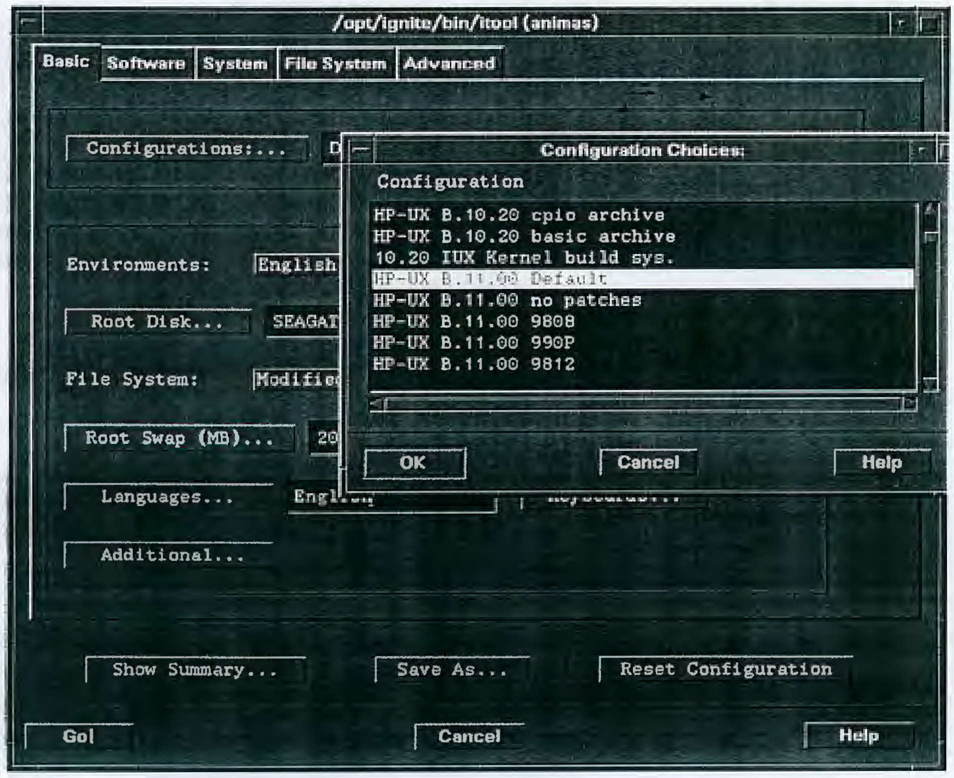
You can build your own config files to specify a particular building block you are interested in, and then combine them in arbitrary ways. Place these building block config files in:
/var/opt/ignite/data/Rel_*release*/*

The next section describes how multiple config files can be combined to define a single configuration.

Combining config Files via INDEX Entries

The grouping of config files into useful configurations is accomplished in /var/opt/ignite/INDEX . This file contains a list of valid configurations, each of which is made up of one or more config files. You can view these configurations from the Ignite-UX GUI when installing a new client at the top of the **Basic** tab by selecting:

Actions –> Install Client -> New Install



Environments: English

Root Disk... SEAGAT

File System: Modified

Root Swap (MB)... 20

Languages... English

Configuration

```
HP-UX B.10.20 cpio archive
HP-UX B.10.20 basic archive
10.20 IUX Kernel build sys.
HP-UX B.11.00 Default
HP-UX B.11.00 no patches
HP-UX B.11.00 9808
HP-UX B.11.00 990P
HP-UX B.11.00 9812
```

For example, the INDEX file might contain:

```
cfg "HP-UX B.10.20 Default"  {
     description "This selection supplies the default system
       configuration that HP supplies for the B.10.20 release.”
     "/opt/ignite/data/Rel_B.10.20/config"
     "/var/opt/ignite/data/Rel_B.10.20/core_700_cfg"
     "/var/opt/ignite/data/Rel_B.10.20/core_800_cfg"
     "/var/opt/ignite/data/Rel_B.10.20/apps_700_cfg"
     "/var/opt/ignite/data/Rel_B.10.20/apps_800_cfg"
     "/var/opt/ignite/data/Rel_B.10.20/patches_700_cfg"
     "/var/opt/ignite/data/Rel_B.10.20/patches_800_cfg"
     "/var/opt/ignite/config.local"
}
cfg "CAD System-10.10" {
     description "This selection is the typical CAD system

     installation for HP-UX B.10.10”
     “/opt/ignite/data/Rel_B.10.10/config”
     “/var/opt/ignite/data/Rel_B.10.10/core_700_archive_cfg”
     “/var/opt/ignite/data/Rel_B.10.10/apps_700_cfg”
     “/var/opt/ignite/data/Rel_B.10.10/patches_700_cfg”
     “/var/opt/ignite/config.local”
} = TRUE
```

With this INDEX file, the Ignite-UX would present two configurations: **HP-UX B.10.20 Default** and **CAD System-10.10**. The **CAD System-10.10** configuration is the default (it is marked TRUE). Once you choose one of these base configurations, you can do further customizations with the UI or accept the config defaults and do the install immediately.

If you selected **CAD System-10.10**, you would get the combination of the five config files listed for that clause. The order of the config files is significant; attributes specified in a later config file can override the same attributes specified in an earlier config file. There are also two config files which are implicitly used every time. Any information stored in the first 8KB of /opt/ignite/boot/INSTALLFS is implicitly appended to each configuration. The client-specific configuration file /var/opt/ignite/clients/0x*LLA*/config is implicitly added as the last config file for each configuration.

A default cfg clause for each release is shipped as part of Ignite-UX. Additional cfg clauses are added when you:

- Save a named configuration from the GUI with the **Save As** button.
- Create a configuration by modifying the INDEX file directly.
- Use the manage_index file to help automate INDEX file modifications.

Example Config Files

This section shows a few example config files to give you an idea of their look and capabilities. See the *instl_adm* (4) manpage for a complete description of Ignite-UX config files.

Defining disks

This example shows how a disk might be defined. Here, the disk is located at hardware address 2/0/1.6.0 and does not use LVM or VxVM. The disk contains the / file system and a swap area. The swap area takes up 64 MB and the file system takes up whatever space is left over:

```
partitioned_disk {
    physical_volume disk[2/0/1.6.0]

    fs_partition {
        mount_point ="/
        usage=HFS
        size=remaining
        file_length=long
    }
    swap_partition {
        usage=SWAP
        size=64Mb
    }
}
```

Combining disks to form a single volume group

In this example, two disks are put together to form a single volume group. Two file systems are defined; both are striped across both disks. The first file system, /apps1, is sized by calculating the amount of space required by the software which is to be loaded, and then adding a 30% free-space cushion. The second file system, /apps2 , gets the remaining space on the disks.

NOTE

The following example shows LVM as the volume manager. However, it is also applicable to VxVM if usage=LVM is changed to usage=VxVM.

```
volume_group “appsvol” {
    usage=LVM
    physical_volume disk[2/0/1.5.0] {
    }
    physical_volume disk[2/0/1.4.0] {
    }
    logical_volume “apps1”

         size=30% free
         usage=VxFS
         mount_point=/apps1
         minfree=5
         stripes=2
    }
    logical_volume “apps2” {
        mount_point= “/apps2”
        usage=VxFS
        size=remaining
        minfree=5
        stripes=2
    }
}
```

Defining networking

This example defines a few of the network parameters which will be assigned to the system after it has been installed:

```
final system_name = "acorn1"
final ip_addr["lan0"] = "15.99.45.123"
final netmask["lan0"] = "255.255.248.0"
final nis_domain = "nis1"
final route_gateway[0] = "15.99.45.1"
```

Defining an install depot

This example defines a single SD depot from which software can be installed. Two different pieces of software are defined for the SD depot. Each can be selected independently for installation. The impact lines tell Ignite-UX how much space this software requires in a given directory. This information is used to size the file systems correctly. The sw_category construct allows you to group the software so that the user interface can present it in chunks which make sense to you. Since this example references an SD depot, it would have been created by make_config:

```
sw_source "ee_apps_depot" {   description = "Electrical Engineering
Application"    source_format = SD
   source_type = "NET"
   sd_server = "15.23.45.6"
   sd_depot_dir = "/var/opt/ignite/depots/Rel_B.10.20/ee_apps"
}
sw_category "Applications" {
   description = "User Applications"
}
sw_sel "EE CAD Package" {
   sw_source = "ee_apps_depot"
   sw_category = "Applications"
   sd_software_list = "EECad,r=1.2,a=HP-UX_B.10.20_700"
   impacts = "/var" 90524Kb
   impacts = "/sbin" 1248Kb
}
sw_sel "EE Routing Package" {
   sw_source = "ee_apps_depot"
   sw_category = "Applications"
   sd_software_list = "EERoute,r=2.4,a=HP-UX_B.10.20_700"
   impacts = "/usr" 12568Kb
   impacts = "/var" 26788Kb
}
```

Customizations Based on the Target System

The config file syntax provides a large number of system attribute keywords which describe the target system. Some examples are:

- The size of the disk at the specified *hw_path*:

```
disk[hw_path].size
```

- The amount of memory present on the target system:

  ```
  memory
  ```

- The string returned from **uname -m**:

  ```
  hardware_model
  ```

- The link-level address of the target system:

  ```
  lla
  ```

System attribute keywords can be used in expressions in config files so that a particular clause is only included in specific target situations. The basic format of these clauses is:

```
   (x) {y}
```

which translates roughly to "if the expression *x* is true, then do *y*."

For example, this clause sets the size of some kernel tunable parameters if the target system has more than 256 MB of memory:

```
(memory > 256Mb) {
    mod_kernel += "nproc (20+12*MAXUSERS)"
    mod_kernel += "maxuprc 1000"
}
```

As another example, use this if you want to run a script to do some particular graphics customizations, but you only want to do so when the target system has the appropriate hardware:

```
(graphics[0].planes > 0) {
    post_config_script +=
        "/var/opt/ignite/scripts/multi_plane_graphics"
}
```

You can also specify multiple conditions. This example installs a particular piece of (previously defined) application software if the target system is a workstation (Series 700) having at least two disks. A message lets the user know why it is happening:

```
( (hardware_model ~ "9000/7.*") & (num_disks >= 2) ) {
    note += "Installed apps1 because this is a big series 700."
    init sw_sel "apps1" = TRUE
}
```

It is also possible to add an else clause. This example uses a generic variable capability and mathematical expressions to set the primary swap size based on the amount of memory in the target system:

```
(memory > 512Mb) {
    init _hp_pri_swap = 512Mb
}
else {
    init _hp_pri_swap = memory * 2
}
```

Customizations Based on User Selection

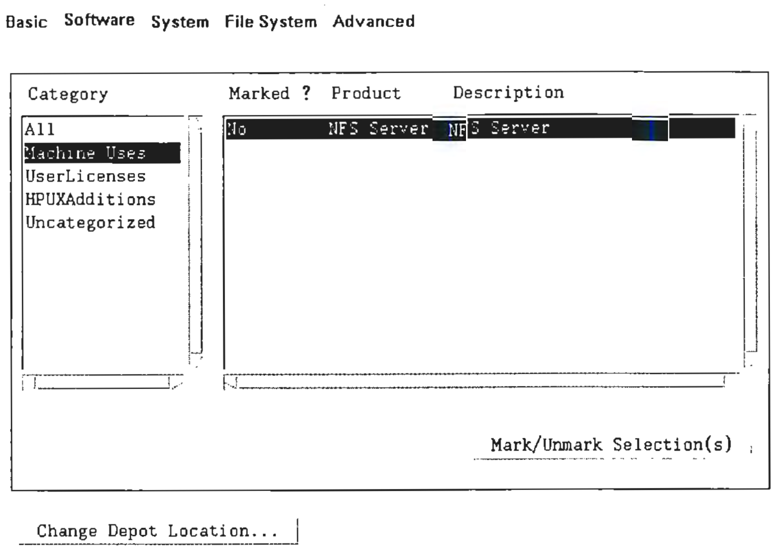
It is sometimes advantageous to be able to select particular customizations independent of the target system's hardware setup. For example, you might have some systems which you intend to use as NFS file servers. You would like the ability to select NFS server capability from the UI when you are configuring the target system.

You have found that NFS file servers are more efficient if some of their kernel parameters are modified. NFS file servers also require some changes to the /etc/rc.config.d/nfsconf file via ch_rc.

One solution is to define a custom software selection with a sw_sel clause, which Ignite-UX shows on the **Actions** –> **New Install** –> **Software** tab when you are configuring a new installation. For example:

```
sw_source "special configs" {
    source_format = cmd
}

sw_sel "NFS Server" {
    sw_category = "Machine Uses"
    sw_source = "special configs"
    mod_kernel += "dbc_min_pct 35"
    mod_kernel += "dbc_max_pct 65"
    post_config_cmd += "
        /usr/sbin/ch_rc -a -p NFS_SERVER=1
        /usr/sbin/ch_rc -a -p NFS_CLIENT=1
        /usr/sbin/ch_rc -a -p NUM_NFSD=8"
}
```

The next figure shows the **Software** tab when the NFS server config file is used. As shown, the selected category is `Machine Uses` as defined in the config file. Choosing a different category would display a different set of software. If you were to select `NFS Server` from this screen, the kernel modifications specified in the config file would be applied during the installation. Likewise, the `ch_rc` commands specified in the config file will be run as part of the installation.



```
Category              Marked ?  Product       Description
All                   No        NFS Server    NFS Server
Machine Uses
UserLicenses
HPUXAdditions
Uncategorized
```

Using install tabs to configure client installations is explained in Chapter 5, “Installing HP-UX with Ignite-UX on Clients from a Server.”.

Debugging config Files

Designing a config file to meet your needs can be a very tedious task. It usually requires a lot of trial and error. Beginning with Ignite-UX version A/B 2.2.4 (May 2000), the `instl_dbg` command is available to help you with config file design. With the `instl_dbg` command you can:

- Parse a client's configuration files for syntax errors.
- Place all relevant configuration information into one file for review.
- Display and set variables, software selections, and use models.
- Detect any other errors that may occur during a client installation due to faulty configuration files, such as missing software depots/archives.

After you have developed a new config file, run `instl_dbg` from the Ignite-UX server to parse the specified client's config file as well as any of the server's configuration files referenced by the client's config file. `instl_dbg` first scans for any syntax errors. After syntax is checked, `instl_dbg` substitutes variables, use models, and software selections (`sw_sel`) with real values, and writes a single, unified config file if the `-f` option is specified. You can then compare this file with your original to determine required changes, or use this file as is to install the client. More options are available for more thorough checking or to provide more detail.

Example uses

To debug a client system1 config file and print the debugged config file to stdout and save the debugged config file to `system1_cfg.out`:

```
instl_dbg -D /var/opt/ignite/clients/system1 -d -f
system1_cfg.out
```

Debug the config file for the client named system1, show the effects upon the disk layout when the value of `_hp_disk_layout` and `_hp_pri_swap` are changed, and print the "very, very verbose" (`-vvv`) output to the screen as well as the verbose output to `system1_cfg.out`:

```
instl_dbg -D /var/opt/ignite/clients/system1 -d \
-V _hp_disk_layout="Whole disk (not LVM) with HFS" \
-V _hp_pri_swap=500MB -vvv -f system1_cfg.out
```

Additional examples can be found in the *instl_dbg* (1M) manpage.

4 Installing HP-UX with Ignite-UX on Clients Locally

You can install the client locally by **pulling** the HP-UX operating system from an Ignite-UX server in **terminal user interface** (TUI) mode, as explained in this chapter.

For multiple target installations, you will generally be executing the installation from an Ignite-UX server. Ignite-UX allows you to install one or more client systems manually from the Ignite-UX screen as explained in Chapter 5, from a remote system by using bootsys which is also in Chapter 5, or automatically as explained in Chapter 10. These are called **pushing** installations.

Both installation methods, pushing or pulling, require that a configuration (config) file be created, as explained in Chapter 3. The configuration can include any supported HP-UX 10.*x*, 11.0, or 11i OS, plus any required patches and applications.

This chapter discusses the steps for installing HP-UX on client systems locally. Topics are:

- Preparing Clients for Installation.
- Non-Interactive Installation Using bootsys.
- Booting Client Systems from the Network.

Preparing Clients for Installation

Boot each Series 700 or Series 800 client system that supports network boot either by entering the appropriate command explained in the following pages or by using the Ignite-UX screen. If a client with a known IP address is already running HP-UX, you can use the `bootsys` command (see page 65) from the Ignite-UX server to install a specific configuration without further interaction.

TIP To interrupt the boot process on any HP computer system, press **Esc** on the given system.

The next section provides a brief review of the manual boot process. Boot ROM commands for manual booting are explained in the installation guide supplied with the HP-UX OS/OE media:

- *Installing and Updating HP-UX 10.x, Chapter 3.*
- *HP-UX 11.0 Installation and Update Guide*
- *HP-UX 11i Installation and Update Guide*

If the client cannot find the server to boot from, check these items:

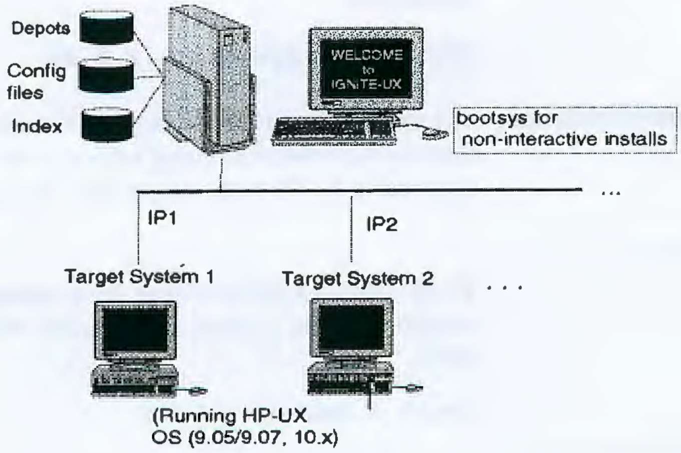
- Client is on the same subnet as the server.
- Any `instl_bootd` errors in: `/var/adm/syslog/syslog.log`
- The `/var/adm/inetd.sec` file to make sure that IP address `0.0.0.0` is not being disallowed.
- If `/etc/services` comes from NIS, make sure that the NIS server has `instl_boot*` entries.

The icons for all clients booted from the Ignite-UX server should now appear on the Ignite-UX client/server screen. If the Ignite-UX server has not been set up completely, or if the client could not obtain enough networking parameters via DHCP, then the client may require interaction on the Ignite-UX client/server screen.

Now that you can view clients on the Ignite-UX client/server screen, you can proceed to Chapter 5.

Non-Interactive Installation Using bootsys

You can use bootsys to start an interactive system installation on one or more clients without logging onto the client system, as illustrated in the following diagram.



It can be invoked either from a command shell, or from the Ignite-UX screen by selecting:

Actions –> Boot Client

Each client must:

- Be currently booted under HP-UX 10.20 or later.
- Be accessible on the network.
- Have enough disk space in the /stand directory to hold these files:

  /opt/ignite/boot/INSTALL

  /opt/ignite/boot/INSTALLFS

bootsys copies the Ignite-UX kernel and RAM file system to each client and then sets the system AUTO file in the LIF area of the root disk to automatically boot from this kernel at the next system reboot.

Examples

This sample command will boot the client system from the boot1 server and wait for install instructions from the Ignite-UX server:

```
bootsys -w boot1
```

If you have already run an install session from the server, issuing `bootsys` without the `-w` option results in automatic installation without further intervention.

To automatically install `system1` using a different IP address than what is currently assigned and without waiting for server interaction, use this command:

```
bootsys -a system1:1.2.3.45
```

More information...

See the *bootsys* (1M) manpage for more information and examples. Common problems using `bootsys` with Ignite-UX are covered in Appendix A, “Troubleshooting,” on page 233.

TIP

To prevent a critical client from being inadvertently booted via bootsys, create the file, `/.bootsys_block`. For example, you can create the file with:

```
touch /.bootsys_block
```

Booting Client Systems from the Network

NOTE

Network boot applies to HP Workstations and HP servers except D, K, and R-class servers that do not support the remote network booting feature. For more details on supported systems, see “Ignite-UX Hardware Requirements” on page 25. See Appendix A “Booting older workstations” on page 239 for more information.

This section provides an overview of booting HP computer systems if you have HP computer systems that may not be running HP-UX.

If you need further help with the boot process, enter:

```
BOOT ADMIN> help boot
```

If the client system is already running an OS, use this procedure or the bootsys command as described in the previous section.

Step 1. Determine your network server address for the install. If necessary, see your system administrator for this information.

Step 2. Turn the power ON for the target system.

Step 3. When you see a message about stopping the boot search, quickly press and hold **Esc** down to stop the boot-selection process.

Booting Current Workstations and Servers

After the power is turned on, you will see a GUI screen (workstations) that displays instructions to press **Esc** to stop the boot process. (On servers, the TUI is used.)

Step 1. Press **Esc** to view the BOOT ADMIN menu:

```
Command                                    Description
-------                                    -----------
Auto [boot|search] [on|off]                Display or set auto flag
Boot [pri|alt|scsi.addr] [isl]             Boot from primary,alternate or
SCSI
Boot lan[.lan_addr] [install] [isl]        Boot from LAN
Chassis [on|off]                           Enable chassis codes
Diagnostic [on|off]                        Enable/disable diagnostic boot
```

```
mode
Fastboot [on|off]                        Display or set fast boot flag
Help                                     Display the command menu
Information                              Display system information
LanAddress                               Display LAN station addresses
Monitor [type]                           Select monitor type
Path [pri|alt] [lan.id|SCSI.addr]        Change boot path
Pim [hpmc|toc|lpmc]                      Display PIM info
Search [ipl] [scsi|lan [install]]        Display potential boot device
Secure [on|off]                          Display or set security mode
------------------------------------------------------------------
BOOT_ADMIN>
```

Step 2. If your network only has one Ignite-UX server available, enter:

```
BOOT ADMIN> boot lan install
```

Step 3. Otherwise, to make sure you boot from the correct server, either make the system search for servers and pick one or explicitly tell the system where to boot, as follows:

1. To search for servers type the following (workstations only):

   ```
   BOOT ADMIN> search lan install
   ```

2. The list of servers will be displayed with IP addresses. You may need to run the `nslookup` command on another running system to determine which address corresponds to your Ignite-UX server, if this information isn't already available.

3. Once you know the IP address of your server (as provided by the search or the `nslookup` command), boot the system by entering:

   ```
   BOOT ADMIN> boot lan.nn.n.nn.n install
   ```

   where: *nn.n.nn.n* is your server's IP address.

   The system then begins to load the install kernel from the network server. This should take 3 to 5 minutes.

Booting Older Series 700 Workstations

On older Series 700 systems, you will eventually see this menu:

```
b)    Boot from specified device
s)    Search for bootable devices
a)    Enter Boot Administration mode
x)    Exit and continue boot sequence
?)    HelpSelect from menu:
```

Do one of the following:

- If your network has only one install server and your system is not configured as a diskless client, then type:

  `boot lan`

  The boot may fail the first time because of an intentional delayed response by the install server. If it fails, try it again. If it fails more than three times, check for problems on the install server (see Appendix A, Troubleshooting,) *OR...*

- If your network has multiple install servers, make sure you boot from the network server address specified by your system administrator.

Search for servers

Step 1. Enter: `BOOT ADMIN>` **`search lan`**

Step 2. If your Ignite-UX server does not appear during the search, exit by entering: **`x`**

1. If necessary, enter the search command again:

   `BOOT ADMIN>` **`search lan`**

TIP

It typically takes two or three searches before the Ignite-UX server will be found, due to a built-in delayed response from the server system.

2. Identify your LAN server from the listing.

3. If three attempts result in no response from the desired server, see Appendix A, "Troubleshooting," on page 233.

Step 3. If you know the Ethernet™ address of your server and can specify where to boot without going through the search process, enter:

`BOOT ADMIN>` **`boot lan.080009-`***`nnnnnn`*

where: `080009-`*`nnnnnn`* is the Ethernet address of the install server. (Some newer systems may not use the `080009` prefix.) This number can be found by running the `lanscan` command on the server.

Step 4. If your server is listed during the search, you can boot the system by entering p and the index number of the server. For example:

```
BOOT ADMIN> p1
```

This will cause the boot to begin. Or, exit this screen by entering:

```
BOOT ADMIN> x

BOOT ADMIN> boot p1
```

IPF Client Network Booting Option

Step 1. From the EFI Boot Manager menu, you will see a prompt to select a boot option. Select **Boot option maintenance menu**.

```
EFI Boot Manager ver 1.10 [14.54]  Firmware ver 0.0 [4209]

Please select a boot option

    EFI Shell [Built-in]
    Boot option maintenance menu
    Security/Password Menu (*** Prototype ***)

Use up and down-arrows to change option(s).
Use Enter to select an option
```

Step 2. The Main Menu appears and prompts you to choose an operation. Select **Add a Boot Option**.

```
EFI Boot Maintenance Manager ver 1.10 [14.54]

Main Menu. Select an Operation

        Boot from a File
        Add a Boot Option
        Delete Boot Option(s)
        Change Boot Order

        Manage BootNext setting
        Set Auto Boot TimeOut

        Select Active Console Output Devices
        Select Active Console Input Devices
        Select Active Standard Error Devices

        Cold Reset
        Exit
```

Step 3. The following menu displays. Select an appropriate network card for network boot. For example, look for entries with a MAC followed by the Mac/*LLA* address of the LAN card.

```
EFI Boot Maintenance Manager ver 1.10 [14.54]

Add a Boot Option.  Select a Volume

    Removable Media Boot
[Acpi(HWP0002,0)/Pci(2|0)/Ata(Primary,Maste
    Load File [EFI Shell [Built-in]]
    Load File [Acpi(HWP0002,0)/Pci(3|0)/Mac(00306E1E4ED4)]
    Load File [Acpi(HWP0002,100)/Pci(2|0)/Mac(00306E1E3ED6)]
    Exit
```

Step 4. Enter an appropriate boot option name at the message prompt. For this example, new boot options are named LAN1 and LAN2.

Step 5. Exit to the main menu. The new boot option will now appear in the EFI Boot Manager main menu.

```
EFI Boot Manager ver 1.10 [14.54]  Firmware ver 0.0 [4209]

Please select a boot option

    SCSI2-HPUX
    EFI Shell [Built-in]
    LAN2
    LAN1
    Boot option maintenance menu
    Security/Password Menu (*** Prototype ***)

Use up and down-arrows to change option(s).
Use Enter to select an option
```

Step 6. Select the new boot option you created. The following is an example of a successful boot using the new boot option.

```
Loading.: LAN1
Running LoadFile()

CLIENT IP: 15.1.52.128  MASK: 255.255.248.  DHCP IP: 15.1.53.37
GATEWAY IP: 15.1.48.1
Running LoadFile()

Starting: LAN1

@(#) HP-UX IA64 Network Bootstrap Program Revision 1.0
Downloading HPUX bootloader
Starting HPUX bootloader
Downloading file fpswa.efi  (371200 bytes)

(c) Copyright 1990-2001, Hewlett Packard Company.
All rights reserved

HP-UX Boot Loader for IA64  Revision 1.671

Booting from Lan
Downloading file AUTO   (528 bytes)
Press Any Key to interrupt Autoboot
AUTO ==> boot IINSTALL
Seconds left till autoboot -   0
AUTOBOOTING...
```

5 Installing HP-UX with Ignite-UX on Clients from a Server

This chapter discusses the steps for installing HP-UX on client systems from an Ignite-UX server. Topics are:

- Methods of Installing Client Systems.
- Installing from the Ignite-UX Server.
- Configuring the Installation.
- Advanced Tab.
- Executing the Installation: Go!.
- Viewing and Printing a Manifest.

Methods of Installing Client Systems

Ignite-UX allows you to install client systems manually from the Ignite-UX screen as explained here, or automatically as explained in Chapter 10. These are called pushing installations. You can also install clients from a remote system by using `bootsys`, as explained at the end of this chapter, or install the client locally by pulling an OS from an Ignite-UX server as explained in Chapter 4.

Each installation method requires that a configuration (config) file be created, as explained in Chapter 3. The configuration can include any supported HP-UX 10.*x*, 11.0, or 11i OS, plus any required patches and applications.

This chapter describes installing from the Ignite-UX server, either using the Ignite-UX GUI or remotely using the `bootsys` command.

Supported Peripherals

All disk drives supported on HP computer systems are supported for installation. Fibre channel, tape devices, and LAN cards are also supported.

Disk arrays can be installed with HP-UX, but the installation tasks do not support configuring an array. See your array documentation for configuration information.

The HP-UX client-side installation tools support VT100 and Wyse 60 terminals, compatible emulations, and all HP terminals.

Network Requirements

If you are loading your server depots or client software from a remote system, your target system will also need a network card. If the target system has multiple LAN cards, select the card that is configured onto the correct network by navigating to the **System → Additional Interfaces** menu. Only one LAN card can be used during the installation, configured on the Ignite-UX screen or handled automatically by `bootsys`.

Your server system will need to be configured. In addition you will need:

- If you plan to perform a network boot for a target client then the server must be on the same subnet as the target system that will be installed. Other options include using a boot-helper system on each subnet from which to boot clients. See Appendix B, "Using a Boot-Helper System," on page 261 to set up a boot-helper system or using the `bootsys` or `make_tape_recovery` commands.
- If you have more than one LAN connection, you must select the one to be used for the install process.

TIP You can only boot over the network from the system's built-in Ethernet interface. FDDI is also supported, but for non-booting only.

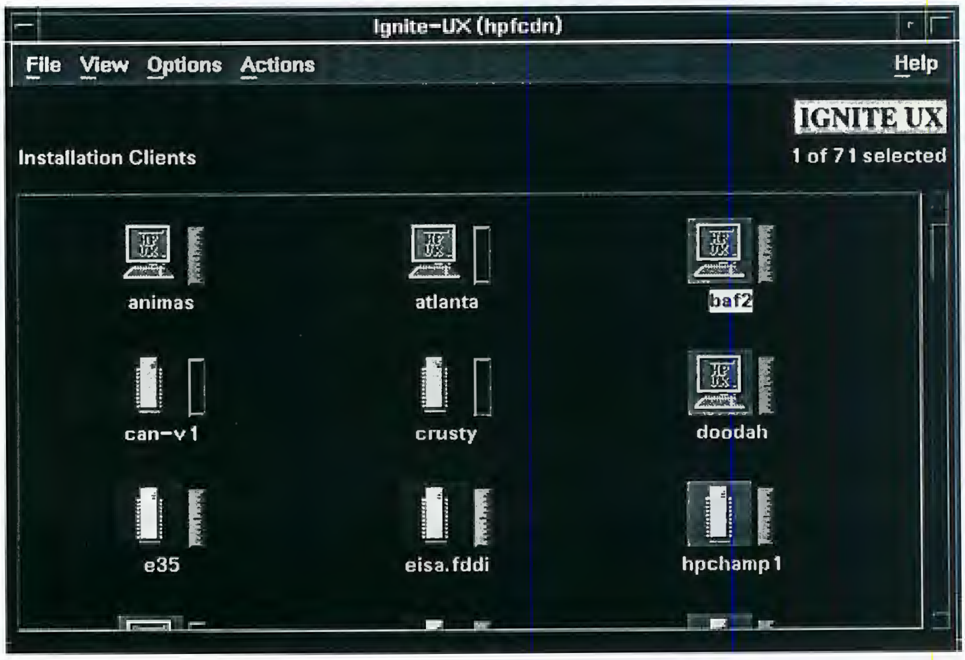
Installing from the Ignite-UX Server

Starting Ignite-UX If you have not already done so, run Ignite-UX on the server as root:

```
/opt/ignite/bin/ignite
```

Running Ignite-UX on the server is explained in the following procedures. Running Ignite-UX remotely from a client or other system provides a TUI with equivalent keyboard navigation.

Ignite-UX screen

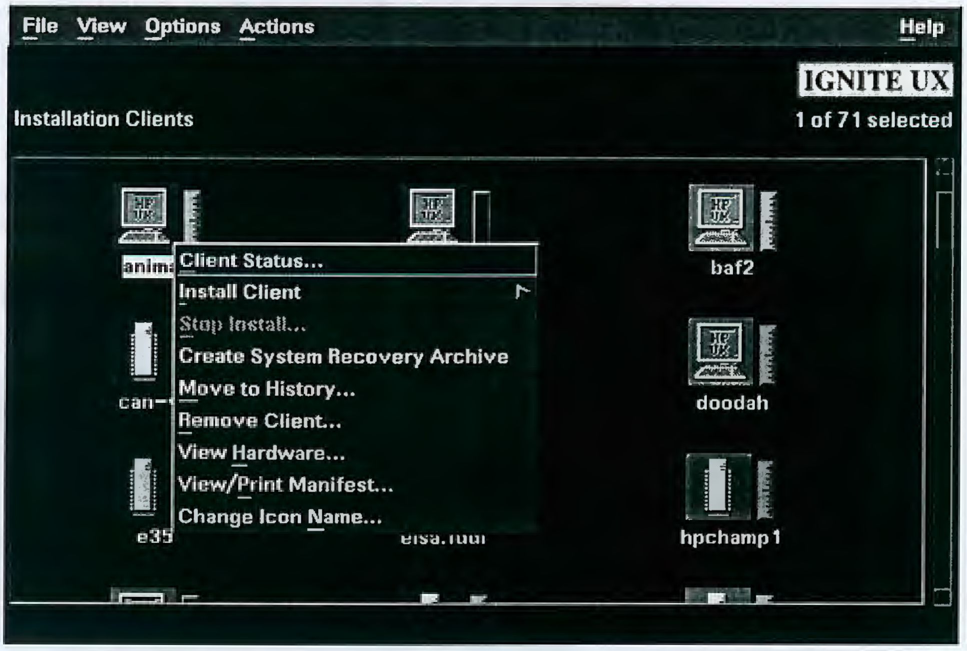


Before any new clients are represented as icons on the Ignite-UX screen, they must first be booted from the Ignite-UX server. If the client is already running an OS, this can be accomplished remotely via the server using: **Actions –> Boot Client**

If the client is not running, see “Booting Client Systems from the Network” on page 67.

After the client icons display, you may:

- Click once on the client icon to select it for further actions.
- Double-click the client icon to get a Client Status screen.
- Right-click the selected client icon to get an Actions menu, which is very similar to the pull-down **Actions** menu:



For more about the available Ignite-UX selections, see Chapter 4, "Installing HP-UX with Ignite-UX on Clients Locally," on page 63 or click **Help**.

Configuring the Installation

To begin the installation, first select a client icon. Then, from the **Actions** menu, select either:

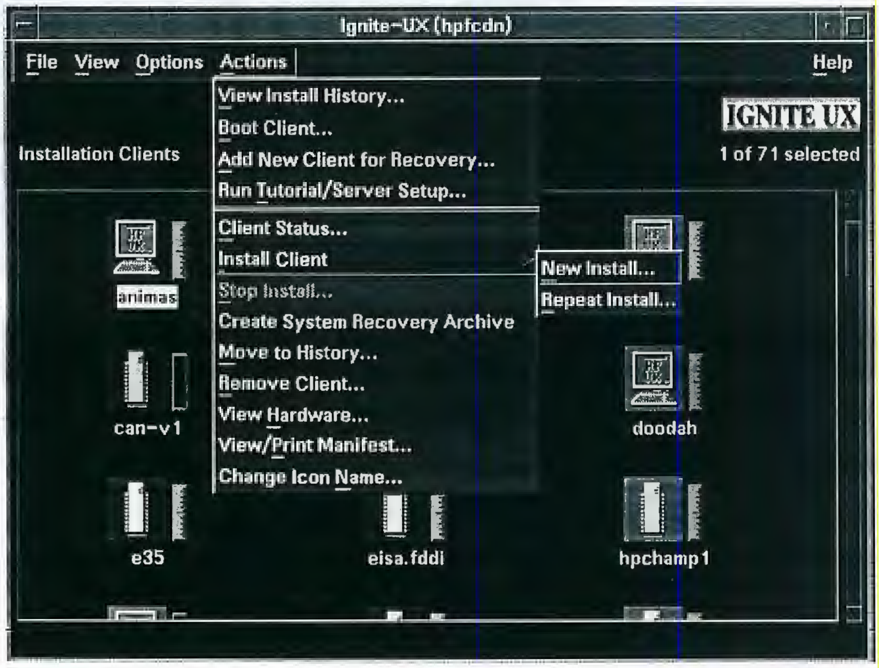
- **Install Client** –> **New install** to install a new client, OR
- **Install Client** –> **Repeat install** to use another clients configuration.

If you have previously installed a client, you will be asked if you want to use the same configuration data again.

If the following message displays:

```
Settings from a previous installation session were found at
startup.  Do you wish to retain these settings for the
current session?
```

Respond **Yes** to re-use some or all of the configuration used in the previous session. Respond **No** to use an entirely new configuration.



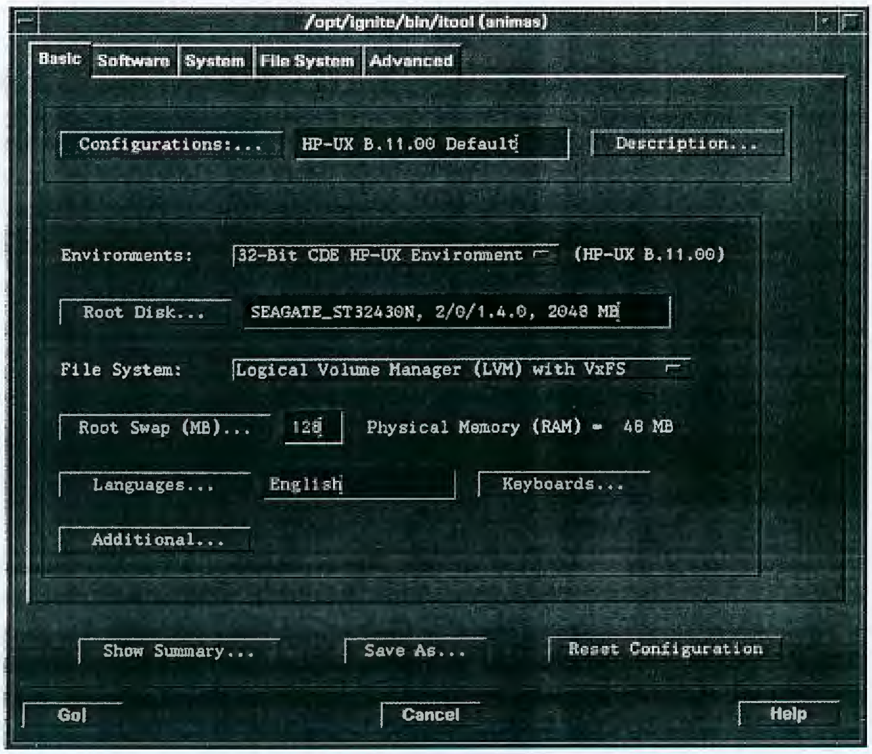
config file parameters

All configuration parameters from an installation are identified and saved as a config file in: `/var/opt/ignite/clients/0x`*`LLA`*`/`

You can use config files in a non-interactive installation using the bootsys command. You can choose a preset configuration in the **Repeat Install** selection list to repeat a previously installed configuration and execute it within Ignite-UX, without further intervention.

Basic Tab

After you choose to install a system, you see the **Basic** screen:



```
Configurations:...   HP-UX B.11.00 Default
Environments:        32-Bit CDE HP-UX Environment   (HP-UX B.11.00)
Root Disk...         SEAGATE_ST32430N, 2/0/1.4.0, 2048 MB
File System:         Logical Volume Manager (LVM) with VxFS
Root Swap (MB)...    128     Physical Memory (RAM) = 48 MB
Languages...         English          Keyboards...
Additional...
```

This screen shows all the basic information for setting up the file system and for loading the OS environment and selecting an HP-UX 11i OE. It also allows you to configure languages, locale, and keyboard requirements. A **Save As...** button also allows saving configurations for later use.

Configurations

Click this selector to display a list of available OS configurations. Then select the one you want to use for this installation. The **Description** button shows more information about each configuration.

Your configuration files are stored in a server location referenced by the `/var/opt/ignite/INDEX` file. The `INDEX` file defines the list of configurations.

OS and HP-UX 11i OE Environments

Select the OS or HP-UX 11i OE environment from the choices available in the list. For HP-UX 11.0/11i, this may include 64-bit or 32-bit OS version. The choices and defaults depend on the releases available on the server, and may include, for example, Common Desktop Environment (CDE) as the default.

File System

Select one of the following:

- **Whole Disk (not LVM)** — This may be the appropriate choice for single-disk systems with disks less than 2GB.
- **Logical Volume Manager (LVM) with HFS** (High-Performance File System) — This selection will format single or multi-disk systems to combine the disk space into a single, large disk pool, and then allocate volumes as needed. The root volume in this case and the swap must be on the same physical volume, and will be configured in this manner by Ignite-UX. The File System tab will provides additional opportunities to configure the LVM volumes. In the File System tab, you can edit the sizes of LVM partitions, or use the values that Ignite-UX computes for you.
- **Logical Volume Manager (LVM) with VxFS** (Veritas File System) — This will format single or multi-disk systems to combine the disk space into a single, large disk pool, and then allocate volumes as needed. VxFS is the same as the Journaled File System (JFS) and allows file system size to be changed after installation. With the optional HP OnlineJFS product you can resize, defragment, or make a "snapshot" of a mounted file system.

- **VERITAS Volume Manager (VxVM) with VxFS** — This will format single or multi-disk systems to combine the disk space into a single, large disk pool, under VxVM, and then allocate volumes as needed. The root, boot, and primary swap volumes must be on the same physical disk and will be configured in this manner by Ignite-UX. The File System tab provides you additional opportunities to configure the VxVM volumes. VxFS is the same as the Journaled File System (JFS) and allows file system size to be changed after installation. With the optional HP OnlineJFS product you can resize, defragment, or make a "snapshot" of a mounted file system.

NOTE VxVM 3.5 is currently only available for HP-UX 11i Version 1.0. VxVM 3.1 is available for HP-UX 11i Versions 1.5 and 1.6.

See "File System Tab" on page 92 for detailed information on File System configuration.

Root disk To change root disks, select this button, select another disk from the list of available disks, and click **OK** in that screen.

For example, a root disk is usually located at SCSI bus location 6.

Root swap The amount of root swap space depends on the applications being loaded. You can choose to use the default which Ignite-UX computes, based on available memory on the target system. Or you can select **Root Swap** and select from the choices that appear in the list. You can also edit the field directly and type in the amount of swap space you wish. The swap will be rounded to a multiple of 4MB or the LVM extent size.

Computing swap space is explained in these HP-UX guides:

- HP-UX 10.*x* — *System Administrator Tasks*.
- HP-UX 11.0 and 11i — *Managing Systems and Workgroups*.

Languages

The languages available in your HP-UX system will be shown when you select this field. Select the item(s) you want, if it is other than the default. The dialogue screen allows you to select more than one language. Highlight the additional items by double-clicking on each. You can also drag the pointer down the screen to highlight a range of items; then press the mark/unmark button.

You can make any of the selections the system default language. This will become the system default language after it is installed.

Locale

Each language will have a corresponding locale (language variant). A locale describes the system management of a language for doing the following:

- Messaging
- Representing numbers
- Displaying monetary values
- Telling time
- Generating characters
- Sorting text

HP-UX can have more than one installed language. The "default language" is the language environment represented on the target system at boot, unless you select another installed language using the HP-VUE or CDE login screen, reset the LANG environment variable, or use geocustoms (HP-UX 10.30 and after) to change it.

Default language choices

Click **Default Language...** to see the **Default Language Choices**. They are listed in two columns: **Language** and **Locale**. Each language may have more than one way of representing itself on the system. If this is the case, there will be multiple locale entries for the same language.

Languages may be activated is several ways:

- **ASK_AT_FIRST_BOOT** allows you to leave the language setting open (unset) until the client system is first booted. At that time, the user will be prompted. The language setting will be performed as part of the initial system configuration. (This applies only to HP-UX 10.30 and later).
- **SET_NULL_LOCALE** creates a NULL language environment, with the locale variables set to NULL by default. A null locale allows programs to execute without using localized message catalogs. This can increase system performance. All HP-UX messages appear in English if the locale is set to **NULL**.

Keyboards... Select the type of keyboard to be used, from the adjacent field. Otherwise, you can use the default selection.

Additional... Click **Additional...** to select among certain pre-configured use-models and variables from your current configuration files. The buttons available are determined from the variables in your config file. When using LVM, you will see selections for easily setting up multiple disks, striping, and file system creation. For details, see the *instl_adm* (4) manpage.

Functions Available on All Tabs

Save as... In server mode, when you have finished your configuration for all tabs, you can save the configuration as a specific file. The saved configurations will then appear under the **Configurations** menu for use in future installations. This function is not available when running the Ignite-UX interface on the install client.

Show summary... Click **Show Summary...** to display the current HP-UX, the basic disk layout, hardware inventory, and other software that will be installed.

Reset configuration Click **Reset Configuration** to change the configuration settings for the currently-selected configuration back to the default settings. You can do this from any tab.

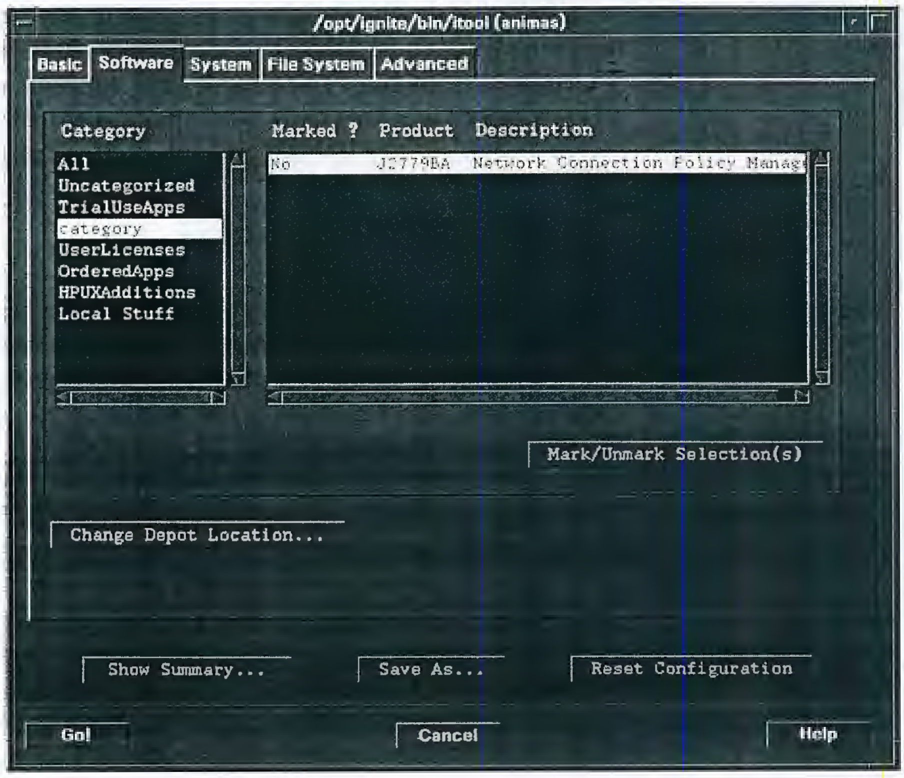
Go! Click **Go!** to initiate an installation. Since **Go!** is always available, click it from any of the tabs. If you don't need to do any customization, click **Go!** now to begin the installation. Then see “Executing the Installation: Go!”, later in this chapter.

After clicking **Go!**, you will still have the opportunity to cancel out of the install sequence.

Cancel Click **Cancel** to exit installing this system.

Help Help information is available on all screens, and you can get context-sensitive help for specific areas by pressing the **F1** function key.

Software Tab



```
Category
All
Uncategorized
TrialUseApps
category
UserLicenses
OrderedApps
HPUXAdditions
Local Stuff
```

```
Marked ?  Product   Description
No        J2779BA   Network Connection Policy Manag
```

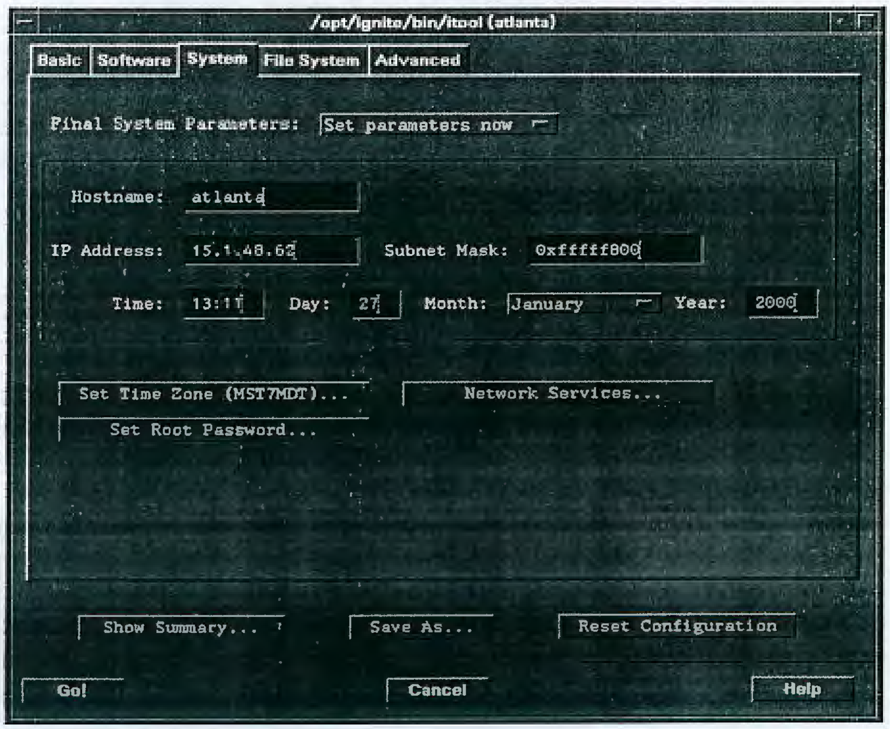
This tab allows you to choose licensing level and additional applications that you configured when you set up your server. To access a specific depot, you can also change depot locations. This display does not dynamically update from a newly-selected depot. When choosing a new depot, it must be identical in content to the current one. If not, use `make_config` on the server to configure the new depot.

- **Category** — Select a topical category to display products available.
- **Product List** — Double-click on a product in the list to select (highlight) it and to toggle its "marked" status (**Yes** or **No**). Alternately, use **Mark/Unmark Selection(s)** to toggle the "marked" status for a selected item.

If patches are kept in a separate depot, by default they are loaded after Core software. If there is more than one non-Core software to be loaded, you may need to specifying the load order for the patch(es) in a config file.

System Tab

You will see a choice selection allowing you to set parameters now, or at first boot of the target system. If you choose to set these parameters now, you see this screen:



Final System Parameters: Set parameters now

Hostname: atlanta

IP Address: 15.1.48.62 Subnet Mask: 0xfffff800

Time: 13:11 Day: 27 Month: January Year: 2000

Hostname

Your system must have a unique system name (a "hostname"), which can be a simple name.

A system name must fulfill the following conditions:

- It must contain no more than eight characters
- It must contain only letters, numbers, underscore (_), or hyphen (-).
- It must start with a letter. Upper case letters are not recommended.

9

- The first component of a host name should contain no more than eight characters, for compatibility with the uname command.

IP address

Use this field to enter the IP address of the form:

n.n.n.n

where: each *n* can be `0` through `255`.

For example:

```
15.1.48.140
```

To determine an existing IP address, use:

`nslookup` ***`hostname`***

Subnet mask

This field sets the subnet mask. The subnet mask will typically be provided by your network administrator, and is of the IP address form or a corresponding hex number. For example:

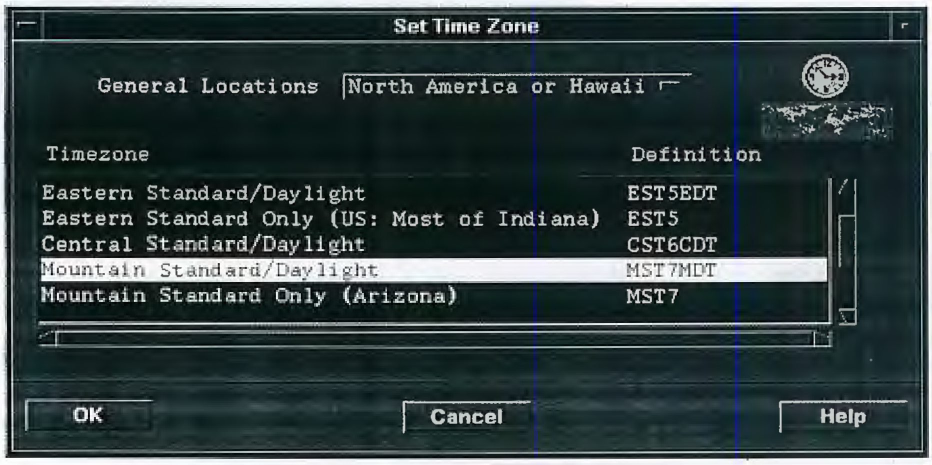
```
255.255.248.0
```

Time and date information

If necessary, enter information for the **`Time`**, **`Day`**, **`Month`**, and **`Year`** fields: For time, use the 24-hour format: *hh*:*mm*

Select the correct month by clicking on the button and selecting from the list. Edit other fields by using the **Backspace** and **Delete** keys.

Set Time Zone screen



Set Time Zone

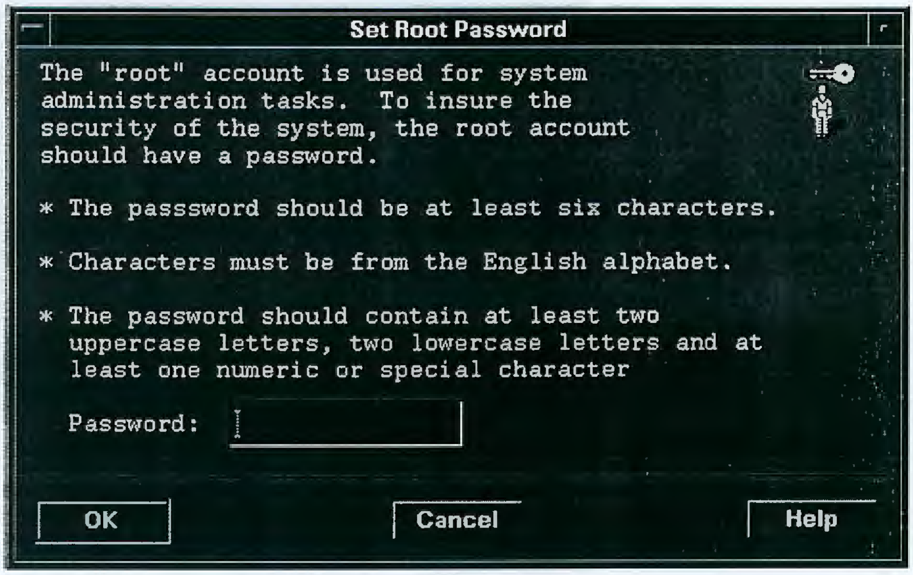
General Locations: North America or Hawaii

Timezone	Definition
Eastern Standard/Daylight	EST5EDT
Eastern Standard Only (US: Most of Indiana)	EST5
Central Standard/Daylight	CST6CDT
Mountain Standard/Daylight	MST7MDT
Mountain Standard Only (Arizona)	MST7

Select this button to bring up a display of time zone selections. You will see two selector lists: the first consists of general locations, and the second has corresponding time zones.

Select an item and click **OK** to make a choice.

Set Root Password screen



Set Root Password

```
The "root" account is used for system
administration tasks.  To insure the
security of the system, the root account
should have a password.

* The password should be at least six characters.

* Characters must be from the English alphabet.

* The password should contain at least two
  uppercase letters, two lowercase letters and at
  least one numeric or special character

  Password:
```

The root account is used for system administration tasks. To insure the security of the system, the root account should have a password.

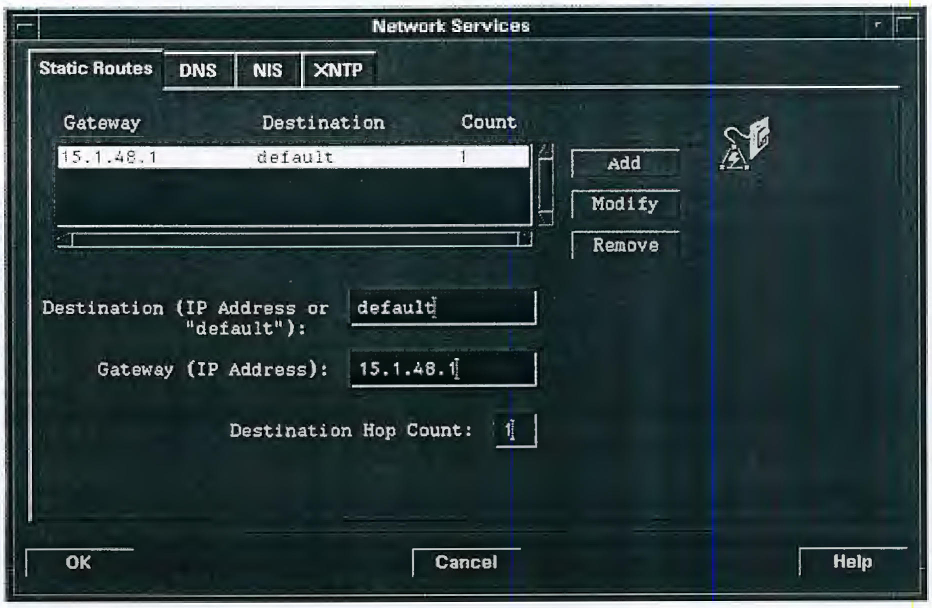
You should observe the following requirements when setting a password:

- The password must be at least six characters long.
- Characters must be from the English alphabet.
- The password should contain at least two uppercase letters, two lowercase letters and at least one numeric or special character.

Network services Click **Network Services** to access tabs used to enter information on:

- **Static Routes**
- **DNS**
- **NIS**
- **XNTP**

Static routes screen



Gateway	Destination	Count
15.1.48.1	default	1

Destination (IP Address or "default"): default

Gateway (IP Address): 15.1.48.1

Destination Hop Count: 1

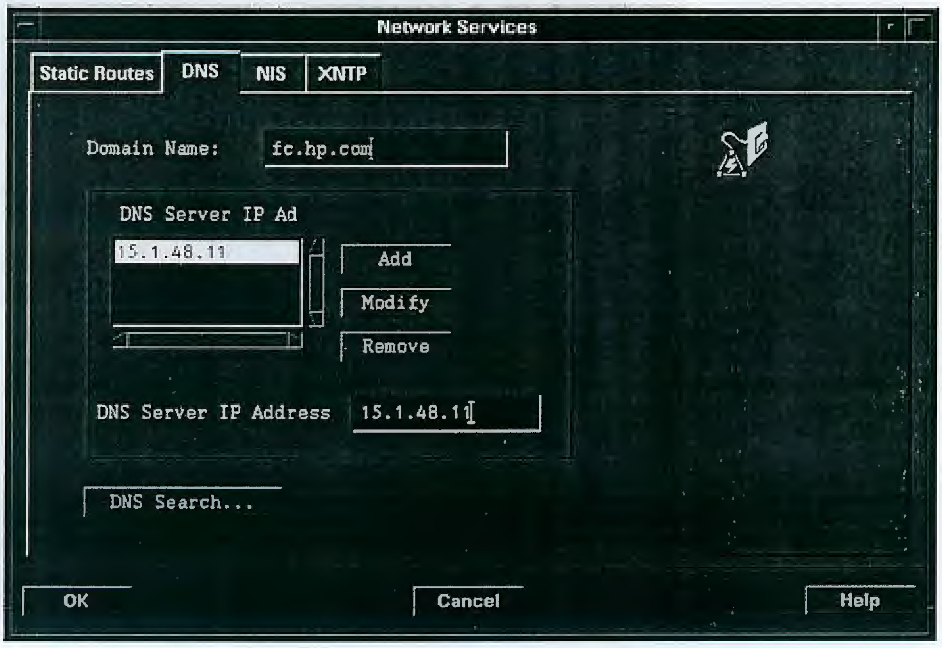
If your network is divided into subnets, you will probably need to specify a gateway system to reach other subnets:

- **Destination** — The field has the word **default** or the IP address of the destination network.
- **Gateway** — The IP address of the device connecting your network to the remote network, or your own IP, if wildcard routing is used.
- **Destination Hop Count** — If your gateway IP is not your system's own IP, this is usually set to `1`. If your gateway IP is the same as your system's, then the Hop Count is `0`.

Once the appropriate fields have been completed on this screen, click the **Add** button.

For more information, see the *routing* (7) manpage.

DNS screen



Domain Name: fc.hp.com

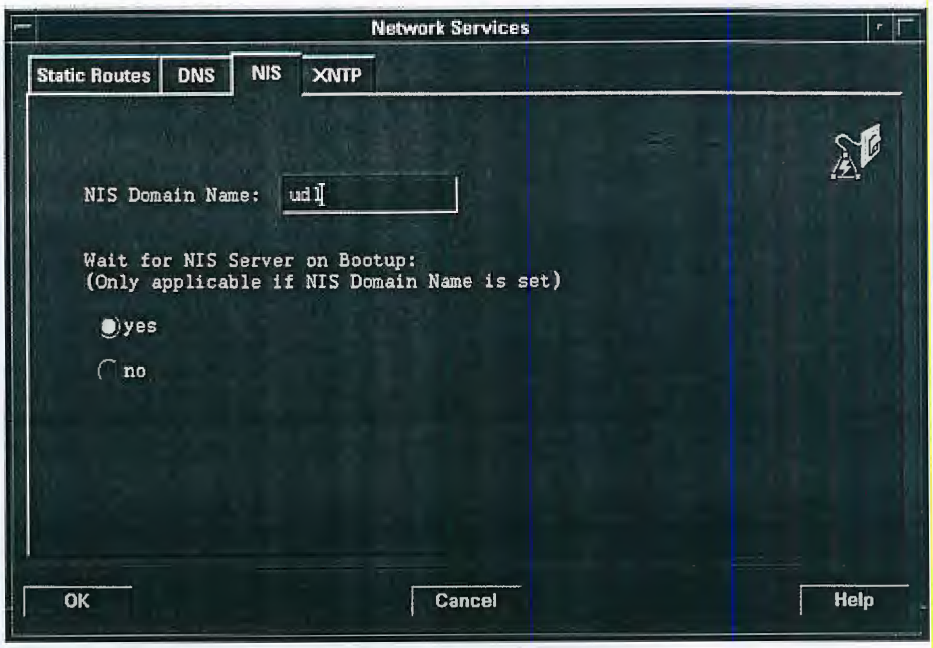
15.1.48.11

DNS Server IP Address 15.1.48.11

On this screen, you can configure the **Domain Name** (an extension to the host name, such as `fc.hp.com`) and the IP address of the Domain Name Server. The listing of current servers is displayed, if they are predefined in the Ignite-UX server. Use the `nslookup` command on a running system to find this information.

After entering a DNS server, click **Add**. Use **Modify** if you are changing an existing entry.

NIS screen



NIS Domain Name: udl

Wait for NIS Server on Bootup:
(Only applicable if NIS Domain Name is set)

● yes

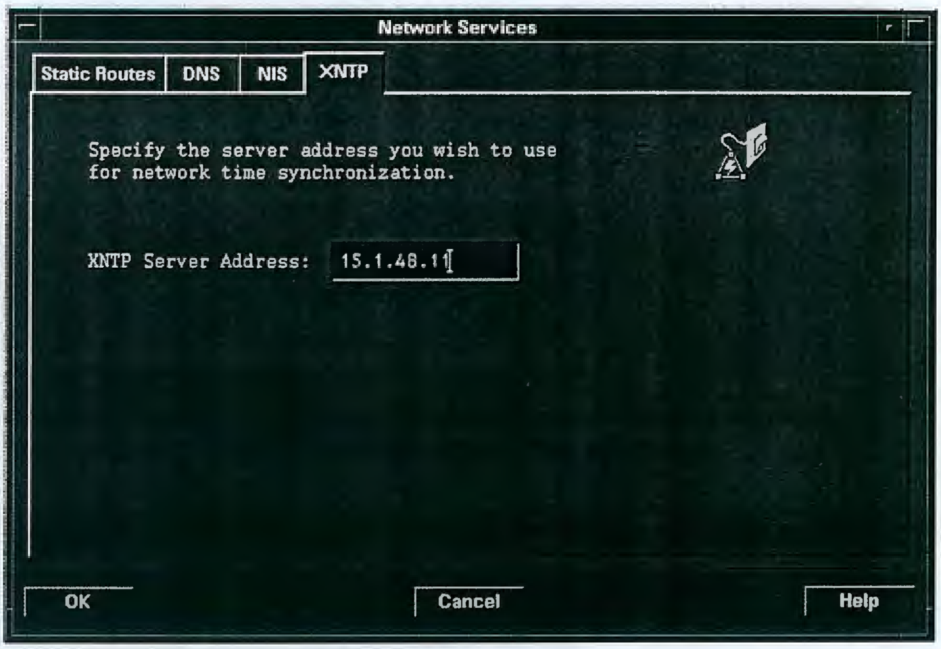
○ no

Typically, the (non-server) hosts in a network are NIS clients. Whenever a process on an NIS client requests configuration information, it calls NIS instead of looking in its local configuration files. The set of maps shared by the servers and clients is called the **NIS domain**.

For more information on NIS, see the *domainname* (1M) manpage or the guide *Installing and Administering NIS Services*.

Wait for NIS server on bootup Select **yes** or **no**, depending on your configuration for NIS.

XNTP screen



```
Specify the server address you wish to use
for network time synchronization.

XNTP Server Address: 15.1.48.11
```

The xntpd daemon maintains system time, in agreement with Internet standard time servers. It does all computations in fixed point arithmetic and clock adjustment code is carried out with high precision.

For more information, see the *xntpd* (1M) manpage.

Additional (network) interfaces

Use this button to bring up a screen for entering information identifying additional LAN interface cards in the target system.

This screen enables you to enter or change IP and Subnet information, as needed, and designate the Primary Interface.

NOTE If the target system has more than one interface, the Primary LAN card will be associated with the host name of the system in `/etc/hosts`.

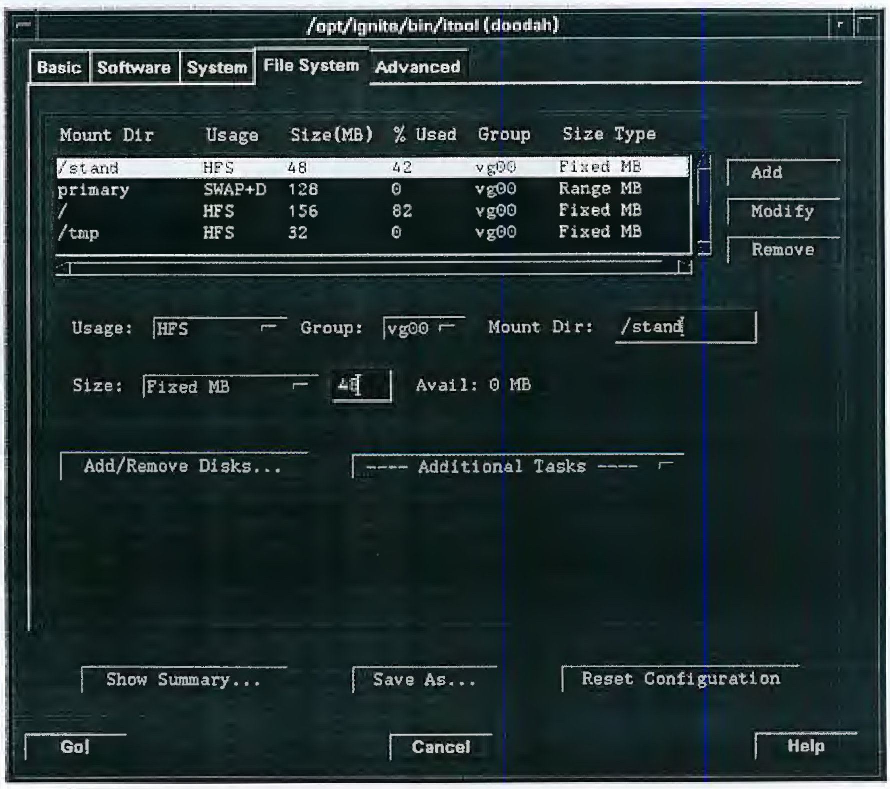
1. Select an **Interface** card from the selection list.
2. Enter or modify the **IP Address**, as needed.
3. Enter or modify the **Subnet Mask**, as needed.

6462 Paula

4. Activate **Primary Interface**, depending on the status you want for this interface.

5. Click **Modify** when you have finished with changes for each interface.

File System Tab



```
Mount Dir    Usage     Size(MB)  % Used  Group   Size Type
/stand       HFS       48        42      vg00    Fixed MB
primary      SWAP+D    128       0       vg00    Range MB
/            HFS       156       82      vg00    Fixed MB
/tmp         HFS       32        0       vg00    Fixed MB

Usage: HFS        Group: vg00    Mount Dir: /stand

Size: Fixed MB    48    Avail: 0 MB
```

This tab enables you to do a variety of file-system and disk-configuration tasks and will differ in appearance, depending on whether you previously selected LVM, VxVM or whole disk, on the **Basic** tab. This illustration is what you would see if you had picked LVM on the **Basic** tab.

Adding and changing file system configuration

To add or change any configurations on the display of file systems:

1. Enter the information in an appropriate field below the display.

2. Select one of the buttons to the right: **Add**, **Modify** or **Remove**.

3. To see more information on the file system display, use the horizontal scroll bar or resize the screen.
4. The **Avail:** indication shows how much space is unallocated in the volume group of the highlighted volume.

For LVM:

- One of the volumes must be root (/).
- A swap volume (primary) is required.
- Directory names must have valid HP-UX names (`/usr`, `/database`, etc.).

For VxVM:

- One of the volumes must be root (/).
- One of the volumes must be boot (`/stand`) with HFS usage.
- A swap volume (primary) is required.
- Directory names must have valid HP-UX names (`/usr`, `/database`, etc.).

The buttons which activate changes are **Add, Modify** and **Remove**.

Generally, changes are not put into effect until you select one of these. If you make a change and then leave the tab without using one of these buttons, your changes may not be applied.

Usage

Select the **Usage** field to see list of file system usage types. If you want to change file system type or usage for the selected item, select an item in this list. The usages are as follows:

- **HFS** — Select this item to create a High-Performance File System.
- **SWAP** — Select this item to create swap.
- **SWAP-Dump** — Select this item to create an area for both swap and system dump.
- **VxFS** — Select this item to create a JFS. This is an extent-based, journaled file system featuring high-reliability, fast recovery time and on-line administration.
- **Unused** — This means the logical volume will be created, but not used.

Group

Click on the **Group** field to open a selection list. You can choose a volume group name from the list.

IMPORTANT

Renaming or changing the disk file-system structure causes the old file system on that disk to be lost (a warning message will remind you of this).

- If you want to add a new/unused disk and give it a different volume group name or create a new volume group, select the **Add/Remove Disks...** field and follow the procedure.
- If you want to reconfigure the volume group in general, including renaming it, click **Additional Tasks** –> **Group Parameters**, where you can fill in a custom group name, and change other disk parameters.
- Click **OK** when you are finished with the sub-screens for any of these tasks. You will be returned to the **File System** tab.

Mount dir

For the root disk, use the standard HP-UX mount directory designations (`"/"`, `"/usr"`, `"/stand"`, `"/var"`, `"/opt"`, etc.) You can also specify your own mount points such as "`/special`" or "`/apps`".

Size

For setting up each selected file system (as shown in the Mount Dir display), the following choices are available:

1. First select an item in the directory display for the file system you want to change. The current selection will show in the **Mount Dir** field.
2. The sizing method (such as "Fixed Size") currently used for that particular file system will appear in the **Size** field. To change the Sizing Method:
   a. Make sure the file system you want to change is selected in the directory display list.
   b. Select the sizing method field to open the list of sizing methods.
   c. Select one of the items (such as **Size Fixed MB**). It will then remain displayed in that field.
   d. Click **Modify** to execute the change on the selected file system.

The types of sizing are:

Fixed The selected (highlighted) file system is set to this size.

All Remaining The selected file system automatically takes over all remaining file system space on the disk or volume group.

Free Size Use this selection when you know how much free space you wish the volume to have after the system is installed. The size of the volume will be the specified amount plus the amount the selected software requires.

Free Percent This category is similar to free size, but expressed in percent. It is used if you know how full you wish the volume to be, in percentage of the volume size. If you indicate "20%", then the volume would be 80% full after the installation of the selected software.

Size Range Select this category in the list to set a maximum size for the file system (the minimum is determined by the software impact on the volume).

NOTE /usr must have sufficient space to accommodate an OS update. The absolute minimum is 324 MB for a 64-bit system. See the installation guide supplied with your HP-UX media.

Add/remove disks This opens a display which allows you to do the following:

- Add a new disk and configure its file system type and volume group designation, if any.
- Remove a disk from current usage on the target system by designating it as **Unused**.
- Determine your current disk usage.

6458
Paula

To change a disk usage status:

- Select a disk in the displayed list.
- Click **Usage** to set a new usage. If you select `LVM` or `VxVM` the **Disk Group**: button appears.
- Click **Disk Group:** to see the volume group choices or type in a new volume group name in the entry field.
- Click **Modify** to execute any changes.

Additional Tasks

This button enables you to configure advanced information in the following categories, as needed. Click on the field to see the following menu items:

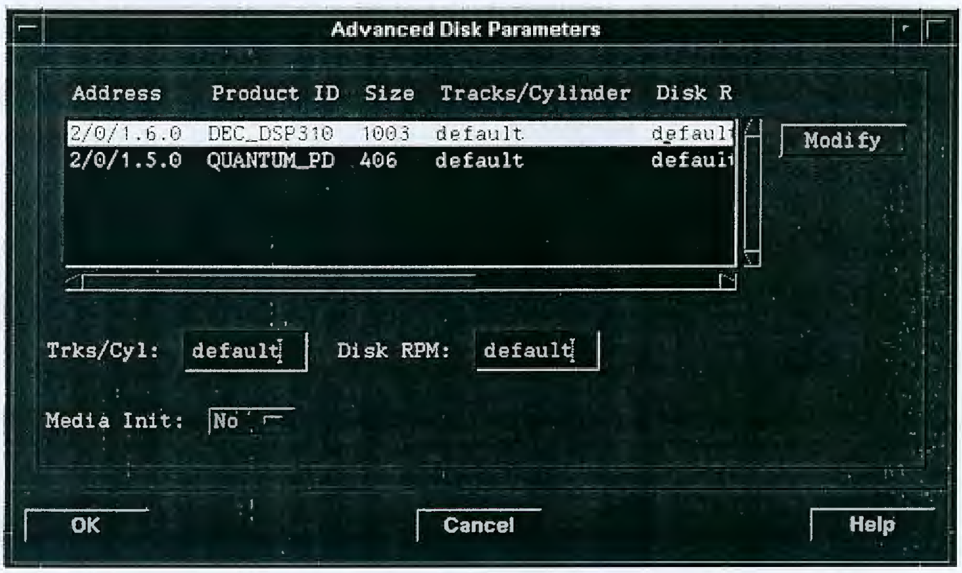
- **Disk Parameters**
- **File System Parameters**
- **Volume Parameters**
- **Group Parameters**

Clicking on one of these will open a screen which will enable you to change advanced parameters. The button will retain the label of the area you are currently working in.

NOTE

Screen choices differ depending on the file system choices you made on the **Basic** tab.

Advanced Disk Parameters screen



```
Address     Product ID  Size  Tracks/Cylinder  Disk R
2/0/1.6.0  DEC_DSP310  1003  default          defaul
2/0/1.5.0  QUANTUM_PD  406   default          defaul
```

Trks/Cyl: default

Disk RPM: default

Media Init: No

Step 1. Highlight a disk in the selection list to select it.

Step 2. Configure the **Trks/Cyl** and **Disk RPM** by direct editing, as needed.

Step 3. Indicate whether Media Init is required by clicking on the selection box and selecting a choice.

Step 4. Click **Modify** to configure changes.

Step 5. Click **OK** to leave **Advanced Disk Parameters** and return to the **File System** tab.

Tracks per cylinder

Step 1. Select a disk by clicking on its entry.

Step 2. Edit the **Trks/Cyl** field as needed and click **Modify** to execute any changes.

Step 3. Click **OK** to leave this screen and return to the **File System** tab.

Disk RPM

Step 1. Select a disk by clicking on its entry.

Step 2. Edit the **Disk RPM** field as needed and click **Modify** to execute any changes.

Step 3. Click **OK** to leave this screen and return to the **File System** tab.

NOTE Running `MediInit` is not recommended unless hardware damage is suspected.

Media init

Step 1. Select a disk by clicking on its entry in the list displayed.

Step 2. Click **MediaInit** to open the selection list.

Step 3. Click **Yes** or **No**. If this is set to **Yes**, you will also see the **Interleave** field.

Step 4. Click **Modify** to execute any changes.

Step 5. Click **OK** to leave this screen and return to the **File System** tab.

More information...

- *mkfs_vxfs* (1M)
- *mkfs_hfs* (1M)
- *mediainit* (1)

Intrlv

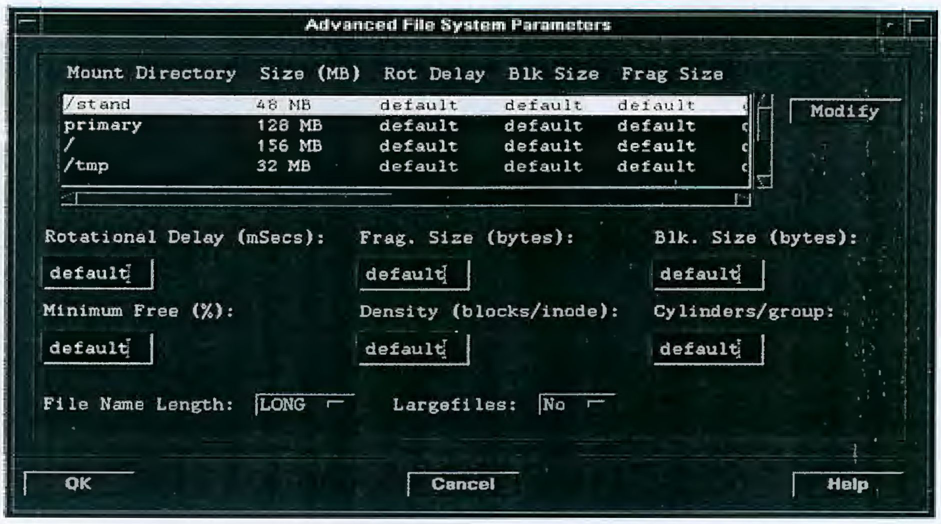
This field is available if **Media Init** is set to **Yes**.

The interleave factor, "interleave", refers to the relationship between sequential logical records and sequential physical records on the disk. It defines the number of physical records that lie between the beginning points of two consecutively numbered logical records. The choice of interleave factor can have a substantial impact on disk performance.

For more information, consult the guide for your disk hardware.

Also see the *mediainit* (1) manpage.

Advanced File System Parameters screen



Advanced File System Parameters

Mount Directory	Size (MB)	Rot Delay	Blk Size	Frag Size
/stand	48 MB	default	default	default
primary	128 MB	default	default	default
/	156 MB	default	default	default
/tmp	32 MB	default	default	default

Rotational Delay (mSecs): default

Frag. Size (bytes): default

Blk. Size (bytes): default

Minimum Free (%): default

Density (blocks/inode): default

Cylinders/group: default

File Name Length: LONG

Largefiles: No

These parameters apply only to HFS file systems:

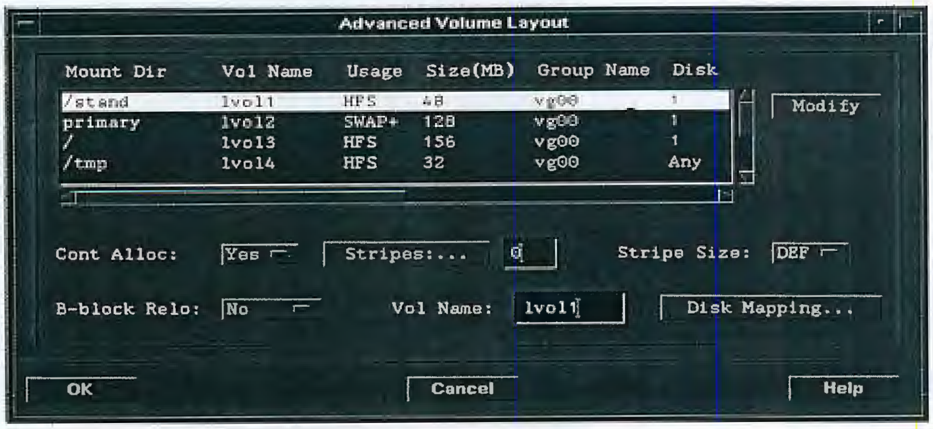
- **Rotational Delay**
- **Fragment Size**
- **Block Size**
- **Minimum Free**
- **Disk Density**
- **Cylinders/Group**

You can use the default values computed by Ignite-UX, or change them, as needed. Selecting **default** means it will use the default defined by the `mkfs` command. When you have finished with this area, click **OK** to return to the **File System** tab.

To get more details, see the *mkfs_hfs* (1M) and *mkfs* (1M) manpages.

6454
Paula

Advanced Volume Layout screen (Volume Parameters)



```
Mount Dir     Vol Name    Usage    Size(MB)   Group Name   Disk
/stand        lvol1       HFS      48         vg00         1
primary       lvol2       SWAP+    128        vg00         1
/             lvol3       HFS      156        vg00         1
/tmp          lvol4       HFS      32         vg00         Any
```

Cont Alloc: Yes   Stripes:... 0   Stripe Size: DEF

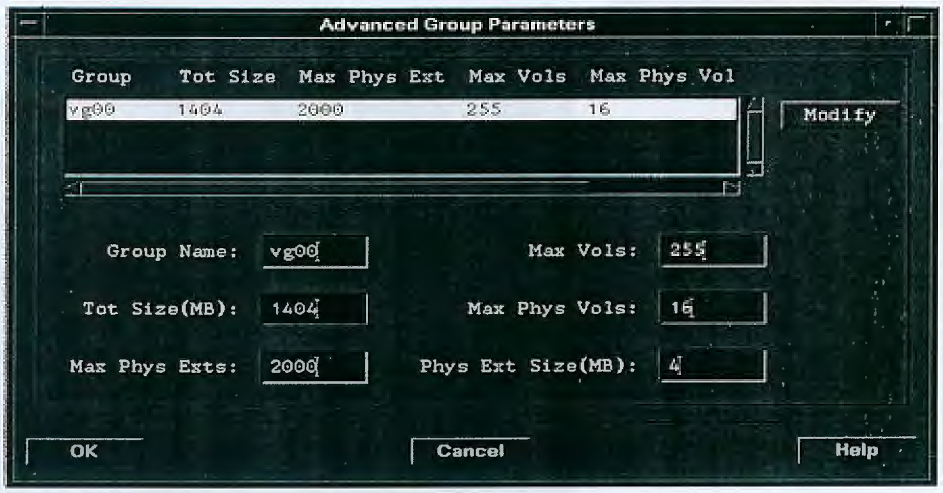
B-block Relo: No   Vol Name: lvol1

Example is shown using LVM.

Use this screen to perform detailed configuration of volumes, as needed, in the following areas. For more detailed information, see the *lvcreate* (1M) manpage for LVM or the *vxassist* (1M) manpage for VxVM.

- **Cont Alloc** — This sets the contiguous allocation policy. A contiguous logical volume has these characteristics:
  - — Physical extents are allocated in ascending order.
  - — No gap is allowed between physical extents within a mirror copy.
  - — Physical extents of any mirror copy all reside on a single physical volume.
  - — The root volume (/), the boot volume (/stand), dump volumes and primary swap must always be created with **Cont Alloc** set to **Yes.**
- **B-block Relo** (Bad-Block Relocation)
- **Stripes** — If two or more disks are in the volume group, then you may enable data striping over multiple disks for performance purposes.
- **Stripe Size** — Configure this if you have at least two disks in a volume group. The default stripe size is 64Kb.
- **Vol Name** — Enter the name you want for the selected volume.
- **Disk Mapping** — Displays a screen which allows you to restrict the disk drives on which the volume data will reside. Normally, the data will be allocated over these disks sequentially.

Advanced Group Parameters screen



Group	Tot Size	Max Phys Ext	Max Vols	Max Phys Vol
vg00	1404	2000	255	16

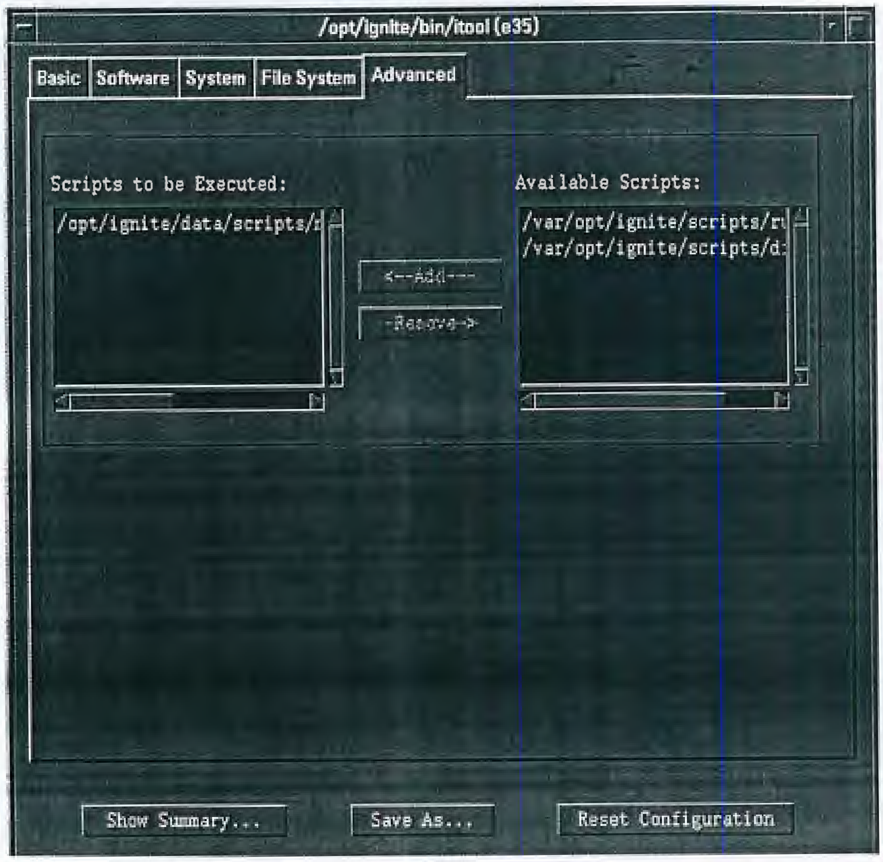
Group Name: vg00
Tot Size(MB): 1404
Max Phys Exts: 2000
Max Vols: 255
Max Phys Vols: 16
Phys Ext Size(MB): 4

Example is shown using LVM.

Use this screen perform detailed configuration of volumes, as needed, in the following areas. For more detailed information, see the *vgcreate* (1M) manpage for LVM or the *vgdg* (1M) manpage for VxVM.

- **Group Name** — Use to rename existing volume groups.
- **Max Vols** — Maximum number of logical volumes.
- **Total Size** — Total size of all volumes.
- **Max Phys Vols** — Maximum number of volumes.
- **Max Phys Exts** — Maximum physical extents.
- **Physical Ext Size** — Physical extent size in MBs.

Advanced Tab



```
/opt/ignite/data/scripts/r
```

```
/var/opt/ignite/scripts/r
/var/opt/ignite/scripts/d
```

Use this screen to activate any HP or custom scripts which you might want to run as part of your installation. Note that the scripts listed are those with a "scripts" keyword in the `/var/opt/ignite/INDEX` file.

Adding a script To add an item, select the item from **Available Scripts** and click: **Add**

Removing a script To remove an item, select the item in **Scripts to be Executed** and click: **Remove**. The item is deactivated, but remains in the **Available Scripts** list.

Executing the Installation: Go!

Select **Go!** in any Ignite-UX tab to initiate the installation. You do not need to examine all tabs, if you simply want to do a generic installation.

A confirmation screen lists disks that will be written on during the installation process and a log of any warnings or errors.

- If you do not wish to proceed with the installation at this time, click: **Cancel**
- The pre-install analysis display screen is scrollable. Be sure to inspect this information and check to see that the disk(s) described in the display list is the one you intend to install on.
- Any errors which are listed must be corrected before you proceed.

As the installation proceeds, you will see a log including the warnings and errors which may need to be addressed before proceeding.

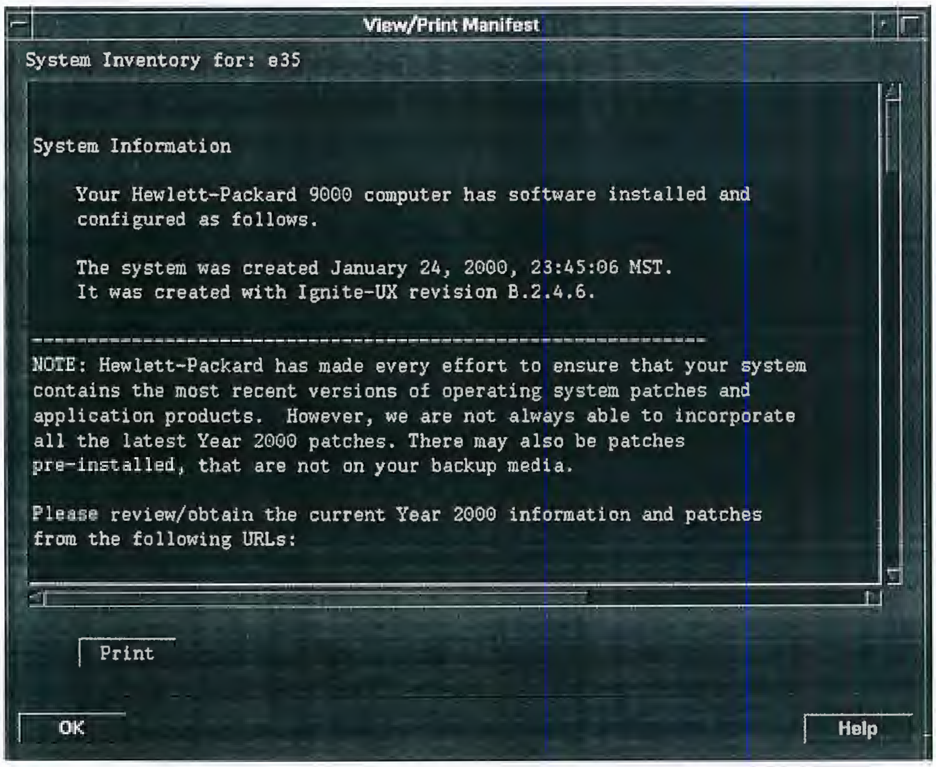
When the installation is complete, you can print a manifest. Then either save the client data in a history directory, remove the client and its data from the server, or just leave the data on the server.

6450
Paula

Viewing and Printing a Manifest

From the Ignite-UX screen

To view a system manifest from Ignite-UX, select a client icon and click: **Actions -> View/Print Manifest**. This is also available from the Client Actions menu (right-click on client icon). The system search may take a moment.



```
System Inventory for: e35

System Information

    Your Hewlett-Packard 9000 computer has software installed and
    configured as follows.

    The system was created January 24, 2000, 23:45:06 MST.
    It was created with Ignite-UX revision B.2.4.6.

------------------------------------------------------------
NOTE: Hewlett-Packard has made every effort to ensure that your system
contains the most recent versions of operating system patches and
application products.  However, we are not always able to incorporate
all the latest Year 2000 patches. There may also be patches
pre-installed, that are not on your backup media.

Please review/obtain the current Year 2000 information and patches
from the following URLs:
```

The manifest provides customer order information for the selected target system.

You can view or print the manifest when a target client is "Complete", as indicated by the Client Status screen. The online information is scrollable.

The manifest contains the following information:

- Customer information, if this has been entered on the individual client configuration screen.
- Hardware connected to the system.
- Storage Devices.
- Installed Software.
- Disk layout.
- File System layout.
- Swap Configuration.
- Kernel Configuration.
- System Information.

Using the print_manifest command

To print the system manifest from the server command line, enter:

```
/opt/ignite/bin/print_manifest
```

The ASCII file is printed to stdout using format instructions from the manifest template file (explained below).

Location of manifest files

Manifest files are saved on the server in:

```
/var/opt/ignite/clients/LLA/manifest/manifest.info
```

and on the target client system in:

```
/var/opt/ignite/local/manifest/manifest.info
```

If the client data is moved to history, that data includes both the client's manifest and config file. Both these files can be recalled at a later time.

Customizing manifest output

Add printer formatting — Include the -e option to add PCL control codes to the output, adding bold headings, etc. to the output.

Print an existing manifest file — Include the -s option to use previously stored data, rather than starting a new system search.

Specify a template file —Use the -t option to specify a template file to customize the manifest output to your needs. A sample template file is: /var/opt/ignite/local/manifest/template.def. The template uses pcl3 formatting commands (similar to printf), allowing you to structure the output as desired. To create your template, be sure to edit a copy of this file, not the original.

For example, if you want a condensed, machine-readable output, you can remove all blank lines and headings from your template. This will also speed-up the manifest generation. This command prints a condensed manifest using the existing manifest file and referencing a template you created named condensed.def:

```
print_manifest -s  -t
/var/opt/ignite/local/manifest/condensed.def
```

You can also access the raw manifest data via a script or program. This file is updated on the Ignite-UX server each time print_manifest is run without the -s option:
/var/opt/ignite/clients/LLA/manifest/manifest.info

6 Installing Patches with Ignite-UX

Ignite-UX uses existing SD depots to distribute software. To distribute patches with Ignite-UX, you need to first bundle them into SD depot format. Patches can be installed along with the Core software being patched.

This chapter shows how to create a patch depot containing HP-UX 11.0 patches, create a single patch bundle of the contents of the depot, and add this bundle to an existing Ignite-UX configuration.

For more details, see the “Managing Patches” chapter in the *Software Distributor Administration Guide* available on the HP-UX Instant Information CD and on the web:

`http://docs.hp.com`

Creating a Patch Depot

Follow these steps to create a patch depot on an HP-UX system.

Step 1. Obtain the set of patches you want to place and manage in an SD depot. For example:

```
PHCO_7891 PHCO_9348 PHKL_9361 PHSS_7726 PHSS_8966 PHSS_9400
PHCO_8353 PHKL_8376 PHKL_9569 PHSS_8667 PHSS_9201
```

HP patches delivered by the Response Center or the web are `shar` files consisting of a serial depot and a `ReadMe` file.

Step 2. Unshar the patches using:

```
for i in PH*
do
sh $i
done
```

Step 3. Combine the separate depots into one depot:

1. Create the directory to store the patches:

   ```
   mkdir /var/opt/ignite/Patches
   ```

2. Copy the individual patch depots into the target depot:

   ```
   for i in PH*.depot
   do
   swcopy -s ${PWD}/$i \* @ /var/opt/ignite/Patches
   done
   ```

Step 4. Verify the contents of the depot:

```
swlist -d @ /var/opt/ignite/Patches
```

Here's the output for the example list of patches above:

```
Initializing...
Contacting target "interop1"...
Target: interop1:/var/opt/ignite/Patches
No Bundle(s) on interop1:/var/opt/ignite/Patches
Product(s):
PHCO_7891 B.10.00.00.AA allows mount to turnon hfs-specific opts
PHCO_8353 B.10.00.00.AA cumulative awk(1) patch
PHCO_9348 B.10.00.00.AA cron(1M) and at(1) patch
PHKL_8376 B.10.00.00.AA Fix vmtrace bug.
PHKL_9361 B.10.00.00.AA Fix panic caused by MP race
PHKL_9569 B.10.00.00.AA NFS and VxFS (JFS) cumulative patch
PHSS_7726 B.10.00.00.AA CDE Dtterm August 96 patch
PHSS_8667 B.10.00.00.AA CDE Runtime Nov96 Patch
PHSS_8966 B.10.00.00.AA LIBCL cumulative patch
PHSS_9201 B.10.00.00.AA fix for aC++ dld.sl
PHSS_9400 B.10.00.00.AA ld(1) cumulative patch
```

The output shows that the depot has "No Bundles." HP-UX Patches are SD "products", but Ignite-UX can only manage SD "Bundles."

Step 5. Convert the individual patches into a single bundle and put the bundle in the Patches depot:

```
make_bundles -B -n Misc_Patches \
-t "HP-UX 11.00 Patches" /var/opt/ignite/Patches
```

Step 6. Rerun `swlist` on this depot to verify that the bundle has been created:

```
swlist -d @ /var/opt/ignite/Patches
```

Here's the output assuming the example patches:

```
Initializing...
Contacting target "interop1"...
Target: interop1:/var/opt/ignite/Patches
Bundle(s):
Misc_Patches HP-UX 11.00 Patches
```

By default, `swlist` shows only the higher level software bundles. This command shows the patch "products" contained in the bundle:

```
swlist -l product -d @ /var/opt/ignite/Patches
```

NOTE If you need to add additional patches to the depot in the future, simply unshar the patches as described above, swcopy them into the Patches depot, and rerun make_bundles. This will repackage the depot.

If you would like to remove a patch from the depot, simply use the swremove command. You can either run swremove and use its friendlier user-interface, or run swremove in command-line mode. This example removes the PHKL_8376 patch from the depot:

```
swremove -d Misc_Patches.PHKL_8376 @ \
/var/opt/ignite/Patches
```

Step 7. If you inadvertently create a bundle of a bundle (for example, if you add an HP product you want distributed with the patch depot), use swremove interactively to examine and delete the extra bundle.

Step 8. Create a config file for the newly-created Misc_Patches bundle. Follow the steps outlined in “Adding a SD Bundle to the Archive Environment” in Chapter 8. Use /var/opt/ignite/Patches for your source depot and specify a new configuration file:

```
make_config -s /var/opt/ignite/Patches -a 700 \
-c /var/opt/ignite/data/Rel_B.11.00/misc_patch_bundle_cfg
```

Step 9. Modify the /var/opt/ignite/INDEX file to include the new bundle in our “HP-UX B.11.0 archive” configuration:

```
cfg "HP-UX B.11.00 archive" {
description "The ARCHIVE B.11.00 release with patches."
"/opt/ignite/data/Rel_B.11.00/config"
"/var/opt/ignite/data/Rel_B.11.00/core_700_archive_cfg"
"/var/opt/ignite/data/Rel_B.11.00/patch_bundle_cfg"
"/var/opt/ignite/data/Rel_B.11.00/misc_patch_bundle_cfg"
"/var/opt/ignite/config.local" }
```

Step 10. To force the installation of the new `Misc_Patches` bundle with the golden-image archive, add this line to the `sw_sel` clause for the patch bundle in `/var/opt/ignite/data/Rel_B.11.00/misc_patch_bundle_cfg`:

```
load_with_any = “golden image”
```

(This file was created with `make_config` in Step 8.)

IMPORTANT Most software distributed by HP, such as applications on DART CDs, are already bundles and will not need (and should not be) bundled again!

6442
Paula

Avoiding Backup Patch Files

When loading HP-UX patches from SD depots, the files that are patched are normally saved, just in case you want to remove the patch at a later date. However, doing this takes up additional space in the /var directory, so you may want to turn this feature off.

The way you control this feature depends on whether you are loading HP-UX 10.*x* or 11.0/11i. It also differs if the patches are coming from the Core depot and being controlled by the hw_patches_cfg config file. See /opt/ignite/share/doc/ace_hwe_setup for more info on hw_patches_cfg.

For HP-UX 10.*x* releases

Control this feature by the existence of the file /var/adm/sw/patch/PATCH_NOSAVE. If you don't want to save the patched files, then you need to have a pre_load_cmd that touches this file. pre_load_cmd can be at the global level or in the sw_source for the patch depot. You can remove this file in a post_load_cmd if you want this feature re-enabled after the load is done. For example:

```
pre_load_cmd += "
   mkdir -p /var/adm/sw/patch
   touch /var/adm/sw/patch/PATCH_NOSAVE"
# Put PATCH_NOSAVE back to the way it was.
post_load_cmd += "
   rm -f /var/adm/sw/patch/PATCH_NOSAVE
"
```

For patches in the core depot that are loaded via the hw_patches_cfg config file, PATCH_NOSAVE is always created and put back the way it was after the core load is complete. See this file for details: /opt/ignite/data/Rel_B.10.20/hw_patches_cfg

For HP-UX 11.0/11i releases

Control this feature by this option in the swinstall command:
-xpatch_save_files=false|true

You can use the sd_command_line keyword, either at the global level or within individual sw_source clauses depending on if you want it specified for all loads or just certain ones.

For patches in the Core depot, this option is specified by the /opt/ignite/date/Rel.B.11.*/hw_patches_cfg file. It is controlled by the config file variable: _hp_patch_save_files and is listed on the Additional Configuration Controls screen.

To specify this option at the global level (for example in the /var/opt/ignite/config.local file), you can add the line:

```
sd_command_line += " -xpatch_save_files=false "
```

To default the variable controlling the Core patches to "NO", add the following to config.local (which must be listed after hw_patches_cfg in the INDEX file):

```
init _hp_patch_save_files = "NO"
```

E6440
Paula
OPL

Avoiding Problems with Superseded Patches

When you are loading HP-UX 10.20 systems from multiple depots that contain patches, it's easy to run into the situation where patches in one depot supersede patches that have already been loaded from another. The superseded patches will prevent themselves from loading by giving an error. Ignite-UX indicates this failure by changing the client icon in the client-server screen to red.

What to do

To work around this problem, use the Ignite-UX `/opt/ignite/bin/fix_patches` script on each depot that contains patches. This script modifies the patch's `checkinstall` script so that it will "EXCLUDE" itself from loading without giving an ERROR.

See `/opt/ignite/share/doc/ace_hwe_setup` for more details. Although there is no manpage for `fix_patches`, enter the following to see command-line syntax:

```
/opt/ignite/bin/fix_patches -?
```

7 Using Golden System Images

This chapter describes how to build and install your own Ignite-UX installation media. Topics include:

- Installing from System Images.
- Creating an OS Archive.
- Configuring Ignite-UX Server to Recognize the OS Archive.
- Enable the Target System.
- Install the OS Archive on the Target.
- Restoring OnlineDiag LIF Volumes.

Examples in this chapter create a **golden system image** or **OS archive**, which is a snapshot of a known, good installation for use to copy to other systems. The copied (source) system is called the golden system image. The OS archive is a compressed tar or cpio archive that will be installed on other client machines.

Ignite-UX does not require creating a golden image to install a new client OS. Installing a golden image, however, is much faster (typically under 30 minutes) than installing the OS via `swinstall`.

6438
Paula

Installing from System Images

In addition to supporting the standard OS installations from an SD depot, Ignite-UX supports installing from system images. This method recognizes that many, if not all, target nodes in a network may be identical (or almost identical) to each other. It is possible to take advantage of this fact by building an archive which contains all of the files you want installed on each of the targets and then using Ignite-UX to install them.

This approach can have several advantages:

- Because the compressed system image is unpacked directly to disk over the network, the installation process can be much faster than an equivalent process using SD. The time savings will depend on the size of the installation being done and the capacity of the network, but a typical system image can be extracted in about 20 minutes compared to about an hour for an SD install.
- Instead of troubleshooting a target, it is often more cost-effective to completely re-install with a known, good system image.
- When coupled with dataless nodes (all volatile data is on a separate file server), system replacement time or move time is drastically reduced.
- Once a system image has been created, it is simple to apply it to multiple target systems. Very little or no user interaction is required during these subsequent installs, reducing the chance of error.

Building this golden system image is done by setting up a single system the way that you want all of your systems to look, and then creating an archive of that system. Follow instructions in this chapter to set up the first system.

Creating an OS Archive

In general, the golden image is simply a system configured with all the software and customizations needed to distribute to a group of target systems. The golden image can be saved on tape or CD from the golden system and installed on individual systems. Or, the golden image can be stored on another system and installed remotely over the network.

Most large HP-UX sites already have the equivalent of a golden system, that is maintained by the IS certification or QA department. This system is configured with customer modifications on top of a base HP-UX system. Critical patches which all users need are installed onto the OS. Local, common software that all users use are also layered on the OS. The resulting system is tested to ensure proper operation in the customer's environment.

These systems represent a prototype or starting point for all users. The steps needed for install customizations are normally captured and are well known. They make good candidates for a golden image archive as explained here. If a golden system already exists, skip to "Configuring Ignite-UX Server to Recognize the OS Archive" on page 121.

Creating a golden system from scratch involves the following steps described in this section:

A. Install the HP-UX OS from media.

B. Load critical patches onto the OS.

C. Load optional HP and third-party software.

D. Customize the system.

Once you have a golden system with the base OS, use Ignite-UX to create an OS archive. It's up to the administrator, to define exactly what constitutes a golden system. You may choose to place patches, applications, kernel configurations, etc. on the golden system, or just include the Core OS. In our example, we only include the Core OS. For speed, you may want to place all of your common applications, patches and tools onto the golden system.

Ignite-UX is capable of installing systems from SD depots and/or archives. You may want to use this capability when setting up your golden system, since you will need to have a system installed before you can get an image.

6436
Paula

A: Install HP-UX OS

Although this can be performed without an Ignite-UX server by using `swinstall` from CD or tape, this example uses Ignite-UX and a network depot as the source of our software.

Step 1. On the Ignite-UX server, set up the Core software to be distributed:

```
make_depots -r B.11.00 -a 700 -s
hpfclc:/release/S700_11.00/B3782EA
/opt/ignite/bin/make_config -r B.11.00
```

`make_depots` copies HP-UX B.11.00 software at the SD depot pointed to by the `-s` option (this pathname depends on the setup of the SD depot you are accessing) onto the local Ignite-UX server. (You can also run `make_config` and point it to the remote depot directly.)

`make_config` then adds this software as a configuration available for Ignite-UX installations.

Step 2. Begin installing HP-UX onto the target golden system by booting the target from the Ignite-UX server:

- If the target is currently running HP-UX, enter:

```
bootsys -v -w -f -i "HP-UX B.11.00 Default" target_hostname
```

- If the target is not currently running HP-UX, enter this on the target console:

```
boot lan install
```

Step 3. Select the configuration you've just set up, "HP-UX B.11.00 Default", and continue with the next section.

B: Load Critical Patches onto the OS

At this point you should have a target system with the basic HP-UX 11.0 release. If you have patches which you wish to distribute to all users, install them now. This is normally done using the standard SD tools.

For example, to install patch PHSS_8375:

Step 1. Download and unshar PHSS_8375 to obtain two files: `PHSS_8375.depot` `PHSS_8375.text`

Step 2. Install the patch non-interactively:

```
swinstall -x autoreboot=true -x match_target=true \
-s /PHSS_8375.depot
```

These instructions can also be found in the `PHSS_8375.text` file.

C: Load Optional Software

Load any optional HP and third-party software you want to make available to *all* users. Keep in mind that we are creating a golden system, and anything put on this will be distributed to all systems installed using the golden image. You'll need to keep in mind licensing restrictions, as well.

HP software (such as compilers) are normally loaded using SD from media or a network SD depot. Third-party software installation varies depending on the vendor.

D: Customize the System

Perform any customizations that you want to distribute to all users. These might include customized CDE login screens, base `/etc/passwd` files, additional phone tools and manpages, or corporate-wide default DNS and NIS setup. It would *not* include system, work-group or site-specific changes such as gateways, user accounts, or machine-specific networking. These will be taken care of by Ignite-UX later.

Use the next steps to create the golden image from the golden system, and configure Ignite-UX to use it. The `make_sys_image` command is provided to assist in creating the OS archive. See the *make_sys_image* (1M) manpage for details.

Step 1. Copy `/opt/ignite/data/scripts/make_sys_image` to `/tmp` on the golden system. Make sure it is an executable file. `/var/tmp` is the default location where `make_sys_image` stores the archive image. You can also have it save the image to a remote server that allows remote access from this client. Whichever method you choose, you will need to have sufficient disk space to hold the image. The amount of disk space will be approximately 1/2 the amount of data contained on your golden system (assuming about 50% compression ratio provided by 1).

6434
Paula

IMPORTANT

Do not use the system while make_sys_image is running in the next step. Device files are removed, and the host and/or networking information on the system are reset. After the command is complete these files are put back.

Step 2. On the golden system, run:

```
/tmp/make_sys_image [options]
```

By default, this will create a gzip-compressed archive in `/var/tmp` with the name *`hostname`*`.gz` , and all specific host information, device files, log files, and network information will be removed. Optionally, if you do not have enough disk space, or you would like for the archive to be created on a remote server, you may use the following options:

```
/tmp/make_sys_image -d directory_to_place_archive \
-s destination_system_IP_address
```

For example:

```
/tmp/make_sys_image -d \
/var/opt/ignite/archives/Rel_B.11.00 -s 15.2.72.150
```

The make_sys_image command can also build an archive containing any combination of tar, cpio, gzip and compress formats. We recommend tar and gzip formats.

Step 3. On the Ignite-UX server, create an archives directory to store the golden image:

```
mkdir -p /var/opt/ignite/archives/Rel_B.11.00
```

The `-p` option creates intermediate directories. It's best to keep the naming conventions `Rel_B.11.00` (or the release you're using.) This directory will need to be NFS exported if you'll be using NFS to transfer the archive to the target.

Step 4. Move the OS archive. For example, if hpfcnjm2 is the hostname: */var/opt/ignite/archives/Rel_B.11.00/hpfcnjm2.gz*

Configuring Ignite-UX Server to Recognize the OS Archive

To create an Ignite-UX configuration file for the OS archive, use the example file: /opt/ignite/data/examples/core11.cfg

Step 1. Create a copy of the example config file:

```
cp /opt/ignite/data/examples/core11.cfg \
/var/opt/ignite/data/Rel_B.11.00/core_700_archive_cfg
```

The destination file name is arbitrary. You can store configuration files anywhere on the system you chose. Ignite-UX manages the names and locations via the INDEX file (see Step 3 below). This file must be accessible via tftp.

Step 2. Modify the core_700_archive_cfg section to set up the OS archive for NFS transfer. Key changes are:

a. In the sw_source clause, change the following:

```
nfs_source =
"15.2.72.150:/var/opt/ignite/archives/Rel_B.11.00"
```

(This points to directory where the archive lives and must be NFS exported.)

b. In the init sw_sel clause, change the following:

```
description = "Archive HP-UX 11.00 CDE"
```

(This will now appear in the Environments section of the Ignite-UX user-interface as a menu choice).

```
archive_path = "hpfcnjm2.gz"
```

(This points to the actual file in combination with the nfs_source line).

c. Add impacts lines in the init sw_sel clause by executing:

```
/opt/ignite/lbin/archive_impact -t -g archive_file
```

6432
Paula

and including the results in the file, replacing the example impacts lines. By default, this assumes that we created a tar archive that was gzipd.

Here is the complete sw_sel clause (some extra clauses in the example have been deleted for simplicity):

```
init sw_sel “golden image” {
description = “Archive HP-UX 11.00 CDE”
sw_source = “core archive”
sw_category = “HPUXEnvironments”
archive_type = gzip tar
# For NFS, the path to the archive is relative to the mount
# point specified in the sw_source:
archive_path = “hpfcnjm2.gz”
# ftp/remsh sources can use a full path:
# archive_path = “/pub/IUXarchives/B.11.00_700_CDE.gz”
impacts = “/” 23Kb
impacts = “/.dt” 35Kb
impacts = “/TT_DB” 18Kb
impacts = “/etc” 1375Kb
impacts = “/export” 1Kb
impacts = “/opt” 74079Kb
impacts = “/sbin” 13449Kb
impacts = “/stand” 1Kb
impacts = “/tmp” 1Kb
impacts = “/usr” 225459Kb
impacts = “/var” 5736Kb
} = TRUE
```

Step 3. Add the new configuration file to Ignite-UX:

Edit the /var/opt/ignite/INDEX file to install a new “configuration” to Ignite-UX. For this example, add a new “cfg” clause as follows:

```
cfg “HP-UX B.11.00 archive” {
description “some description of this archive...”
“/opt/ignite/data/Rel_B.11.00/config”
“/var/opt/ignite/data/Rel_B.11.00/core_700_archive_cfg”
“/var/opt/ignite/config.local” }
```

The line of most interest is the one containing the core_700_archive_cfg, which is the config file we added in Step 2.2. The “config” and “config.local” are standard configurations.

/var/opt/ignite/config.local should be last. The last config file has the highest priority and can override values in prior config files.

The file /opt/ignite/data/Rel_B.11.00/config supplies the disk and file-system layout defaults, plus other control information required by Ignite-UX. It must be first in every cfg clause.

Each cfg clause appears as an available configuration to Ignite-UX. Therefore, the string HP-UX B.11.00 archive will now appear as a valid configuration.

Step 4. Ensure NFS file system is exported correctly.

In the above sw_source clause, we specified the location of the OS archive to be a file on an NFS server. You need to ensure target systems have access to this directory.

Make sure the NFS configuration is correct. To view the current status and ensure the directory containing the archive is correctly exported, enter:

```
exportfs -v
```

Ignite-UX will automatically try to export /var/opt/ignite/clients for its use. In our example, /var/opt/ignite/archives/Rel_B.11.00 must also be exported because that is where we placed the OS archive.

Here's our /etc/exports file:

```
/var/opt/ignite/clients -anon=2
/var/opt/ignite/archives/Rel_B.11.00 -ro,anon=2
```

If these are not correct, use SAM to set them up correctly.

6430
Paula

Enable the Target System

Since the Ignite-UX server now knows about your new OS archive, you can use Ignite-UX to load the OS archive onto a target system. To do this, you need to get the target system to inform Ignite-UX that it is ready to install a new OS. There are two methods for doing this.

Method 1:

If the system is currently running HP-UX 10.x or higher — From the Ignite-UX server, use bootsys to reboot the target for which you wish to install the new OS. The target system can be booted in a mode in which it can be controlled by the Ignite-UX user interface.

```
/opt/ignite/bin/bootsys -w -v system_name
```

This will cause the target system to boot a copy of the Ignite-UX kernel and file system that bootsys copies to the target. An icon representing the system will appear in the Ignite-UX user interface on the server when the system has completed boot. (This may take several minutes.) An icon appears on the Ignite-UX UI when each client is booted.

If the server cannot resolve the system name, specify to bootsys the *system_name* and *IP_address*:

```
/opt/ignite/bin/bootsys -w -v system_name:IP_address
```

Method 2:

If the system does not have an OS — Manually reboot the system. Interrupt the boot process and select the Ignite-UX server as the lan boot source. This command will be slightly different depending on your target system. As an example, to install to a Model 712 workstation, enter the following from the boot admin mode:

```
boot lan.15.2.72.150 install
```

Older Series 700 workstations that use the RMP (rbootd) protocol instead of BOOTP require that you use the hardware LAN address of the server, and omit the install keyword:

```
boot lan.080009-123456
```

Replace the above IP/Ethernet addresses with the correct value for your Ignite-UX server. When prompted with a message about interacting with the IPL, respond **NO**

Install the OS Archive on the Target

In this section, we will use Ignite-UX to customize an OS install. Chapter 9 explains how this can be done with no user/administrator interaction.

Step 1. Run Ignite-UX by executing this as root:

```
/opt/ignite/bin/ignite
```

When the target has rebooted (using either `bootsys` or manual network boot), and is ready for installation, it will appear as an icon, labeled either as its original hostname (if rebooted using `bootsys`), or by the hostname supplied by DHCP, or at Ignite-UX screen.

Step 2. Select or click the icon of the system you wish to install.

Step 3. Select **Actions** –> **Install Client** –> **New Install**

You should now see the Ignite-UX screen with five tabs across the top. (If you see the System Hardware Inventory screen, simply select **OK** to bypass it).

Step 4. In the **Basic** tab (the top tab at startup), select:
Configurations: –> **HP-UX B.11.00 archive**

Ensure that the Root Disk, Root Swap and other fields are correct for your installation. *Any disks you select here will be over-written!* If you have a disk with existing user information you don't want to modify, add it manually after Ignite-UX has installed the OS.

Step 5. In the **Software** tab: Because there is only an archive at this point, the screen is blank. We'll add a patch and application depot later.

Step 6. In the **System** tab, select:
Final System Parameters –> **Set parameters now**
Fill in the blanks with the correct data.

Also fill in the appropriate data under **Set Time Zone, Network Services...** and, optionally, **Set Root Password**

Step 7. In the **File System** tab: Verify the correct disk usage. You can also add disks at this point or modify the disk and file system parameters. *A newfs will be performed on all selected disks!*

Step 8. In the **Advanced** tab: Nothing to specify here at this time. Later, we'll add post-process scripts to execute.

Step 9. When finished entering data, select **Go!** Review the data in the configuration dialog box and select **Go!** again.

Step 10. To display target installation status, double-click the target system icon on the Ignite-UX screen during execution.

Done!

In less than 30 minutes, the target system should have the new OS installed, a new kernel built, and the system rebooted and ready for use. Status of the target system will be shown on its icon, and in the status screen.

When using the Ignite screen

Ignite-UX determines the state of a target by reading the files in the `/var/opt/ignite/clients/`*`LLA`* directory. Seeing an icon on the Ignite-UX screen does not mean that the target actually exists, only that its config and control files exist in the Ignite-UX directories. We can use this behavior to our advantage to reinstall systems. This means that if you are reinstalling a system that Ignite-UX has already installed, you may need to either re-execute `bootsys` or boot the client from the Ignite-UX server.

Restoring OnlineDiag LIF Volumes

To restore OnlineDiag LIF volumes after installing from a golden image, set up a script in the INDEX file to be run as a post-configure script. For example, add this stanza to the /var/opt/ignite/INDEX file:

```
scripts {
   "/var/opt/ignite/scripts/diag.sh"
}
```

The diag.sh script is included as an example script in the /opt/ignite/data/examples directory. It runs this command which copies the OnlineDiag LIF volumes onto the root disk:

```
/usr/sbin/diag/lif/lifload -f /usr/sbin/diag/lif/updatediaglif
```

8 Customizing Your Installation

This chapter shows how to do local customizations using scripts:

- Using Post-installation Scripts.
- Installing Netscape® as a Post-config Step.

Other example uses of scripts to customize installations are in the *make_medialif* (1M) manpage.

Using Post-installation Scripts

Any number of tasks may be performed on the target system after the OS is installed by providing a script to be run on the target system. This section touches on some common examples, but scripts can easily be written to mount additional disk drives, add additional software, modify configurations based on system use, etc.

There are a number of points in the install process in which you can force scripts or commands to be run. Check the “Command and Script Execution Hooks” section on the *instl_adm* (4) manpage for specifics. One point to note is that `post_config_script` will run after all software has been loaded and the system has been booted with its final kernel, but *before* any of the normal `/etc/rc startup` scripts have been run.

Adding a Post-install Script

Example task

1. Create a script to perform the desired task. When Ignite-UX runs this script as a post-configuration, it will be run on the target system.
2. Add the script to your configuration file. Ignite-UX post-configuration scripts are defined using the `post_config_script` variable. For example, you can place this line into your `core_700_archive_cfg config` file:

   ```
   post_config_script += \
   "/var/opt/ignite/scripts/install_default_printer"
   ```

   The line above will define the `install_default_printer` script to be run as a post-installation process on the target system. The line should stand alone, placed *outside* of any clause (such as a `sw_sel` clause). By default, the script will always be run on the targets. You can change the behavior by navigating to **Install Client** –> **New install** –> **Advanced** tab.
3. If you want to make a script available under all configurations, add it to the `/var/opt/ignite/INDEX` file. Add the following to the end of this file:

   ```
   scripts {"/var/opt/ignite/scripts/install_default_printer"}
   ```

   It will then show up in the **Advanced** tab for all configurations.

NOTE Ignite-UX accesses scripts via tftp. Make sure the directory the script resides in is available to tftp by examining and/or changing the /etc/inetd.conf file.

Managing Network Printers

Example task One task an administrator generally needs to perform after a new OS installation is setting up printers. To automate this process, write a script which performs the HP-UX commands for adding a printer. Here is a script for adding a remote printer named “printbob”, and turning on the lp scheduler. The script turns SAM logging on for “commands-only”, performs the tasks desired, and extracts those commands from the SAM log file.

```
#!/sbin/sh
# Post process IUX script to add a local default printer
# Performing task "Add Remote Printer": Adding "printbob"
#
/usr/sbin/lpadmin -pprintbob -ormhpfcmgw.fc.hp.com -orptsslj \
-mrmodel -v/dev/null -orc -ocmrcmodel -osmrsmodel
/usr/sbin/lpadmin -dprintbob
/usr/sbin/accept printbob
/usr/bin/enable printbob
# Turn on lp scheduler
#
lpsched -v
```

Installing Netscape® as a Post-config Step

Here is an example of using Ignite-UX post-installation scripts to load software on new installs. Netscape is one of those tools which seems to have a new version every six months. Due to the frequency of the changes, this tool may not make sense to include on the "golden system".

This example shows one way of accomplishing the task using a `post_config_script`. Another way would be to create a software selection (`sw_sel`) that would reference the tar archive, and then a `post_config_script` (or `post_config_cmd`) associated with the `sw_sel` that would be run only if the selection was picked for loading. Using a `sw_sel` would have the advantage of making it appear in the UI as just another software selection, and would have the `sw_impact` statements to ensure sufficient file system space. For more examples, see the files in `/opt/ignite/data/examples`.

NOTE Be sure the Netscape Navigator product is appropriately licensed prior to installation.

Step 1. Get Netscape Navigator — Netscape Navigator is typically pulled from one of the Netscape ftp server sites. The pulled files are gzip compressed tar images with an encoded name similar to:

```
netscape-v30-export.hppa1.1-hp-hpux.tar.gz
```

Step 2. Special Considerations for Netscape — In order to run Navigator, each user needs the correct network preferences. Unfortunately, these preferences cannot be defaulted, and must exist in every users `$HOME/.netscape` directory. To get around this limitation, we have supplied a "run-netscape" script. Instead of running "netscape", the user can run a link to "run-netscape" which will install the default preferences at first invocation.

A sample "run-netscape" script is shown below. You will also need to create a default configuration file. Merely take an existing one and remove all user and host specific information.

Step 3. Write an install and customization script — Attached below is a script we used for installing Netscape in our environment. The script does the following:

1. Remote copies from a server to the local target netscape, a default-preferences file, and the special run-netscape script.

2. Unpacks Netscape.

3. Makes `/usr/local/bin/netscape` a link to "run-netscape" to ensure user defaults will be installed.

4. Performs the special netscape customization.

5. Cleans up.

We named and placed our script under:

`/var/opt/ignite/scripts/install_netscape`

Step 4. Add the install script to Ignite-UX customization — Add a line like this to one of your config files (not in a clause):

```
post_config_script="/var/opt/ignite/scripts/install_netscape"
```

For details of adding a post configuration script, see Chapter 9. This script will need to be accessible using tftp.

Example script Here's an example post-install script for Netscape:

```
# !/usr/bin/ksh
#
# Post Ignite-UX installation script used to install Netscape
version 3.0.
# This installation assumes HP-UX 11.00 because it
depends on gzip
# already loaded on the system.
#
PATH=${PATH}:/usr/sbin:/sbin:/usr/contrib/bin
IUX_SERVER=interop1.fc.hp.com
IUX_ARCHIVE_DIR=/var/opt/ignite/archives/Netscape
NETSCAPE_GZIP=netscape-v30-export.hppa1.1-hp-hpux.tar.gz
NETSCAPE_INSTALL_DIR=/opt/Netscape
NETSCAPE_RUN_DIR=/usr/local
echo "* Loading Netscape"
mkdir ${NETSCAPE_INSTALL_DIR} cd ${NETSCAPE_INSTALL_DIR}
rcp ${IUX_SERVER}:${IUX_ARCHIVE_DIR}/${NETSCAPE_GZIP}
${NETSCAPE_GZIP} rcp ${IUX_SERVER}:${IUX_ARCHIVE_DIR}/run-netscape
. rcp
```

```
${IUX_SERVER}:${IUX_ARCHIVE_DIR}/default-preferences .
gzip -dc ${NETSCAPE_GZIP} | tar -xvf -
echo "* Finished loading Netscape"# # Configure netscape
runtime # echo "* Configuring Netscape"
chmod 755 ${NETSCAPE_INSTALL_DIR}/run-netscape ln -s
${NETSCAPE_INSTALL_DIR}/run-netscape
${NETSCAPE_RUN_DIR}/bin/netscape
# # Install java_30 # mkdir ${NETSCAPE_RUN_DIR}/lib/netscape
ln -s ${NETSCAPE_INSTALL_DIR}/java_30 \
${NETSCAPE_RUN_DIR}/lib/netscape/java_30
# # Install plugins library # mkdir
${NETSCAPE_RUN_DIR}/lib/netscape/plugins ln -s
${NETSCAPE_INSTALL_DIR}/libnullplugin.so
${NETSCAPE_RUN_DIR}/lib/netscape/plugins/libnullplugin.so
mkdir ${NETSCAPE_RUN_DIR}/lib/netscape/mime.types mkdir
${NETSCAPE_RUN_DIR}/lib/netscape/mailcap
rm -f ${NETSCAPE_GZIP}
echo "* Finished configuring Netscape"
Example run time script for Netscape
#!/bin/sh
# # Put this script in /usr/local/bin/netscape
set -e
# Set this to the location of the real Netscape executable #
REAL_NETSCAPE=/opt/Netscape/netscape
# Set this to the location of the default preferences file. #
DEF_PREFS=/opt/Netscape/default-preferences
if [ ! -e $HOME/.netscape/preferences ]; then echo '(installing
default Netscape preferences...)' mkdir $HOME/.netscape
cp -p $DEF_PREFS $HOME/.netscape/preferences echo '(done)' fi
# The "-name" option is to avoid confusing the users' X resources.
# exec $REAL_NETSCAPE -name netscape $*
```

9 Automating Installations

This chapter shows how to use bootsys and configuration files to automate the Ignite-UX install process.

Setting up your Ignite-UX server so that the default configuration is correct for any given system will save you time and allow you to easily automate installations. This chapter discusses setting up the defaults the way you like them, as well as setting up a configuration for a specific target system.

Ignite-UX can install HP-UX on a target system with no additional configuration information (the default configuration as specified in the /var/opt/ignite/INDEX file will be used). You can, however, select from other configurations listed in the INDEX file on the bootsys command line.

Starting an Automatic Installation with bootsys

To start an automatic installation, enter:

```
bootsys -a -v [-i configuration]  [-f]  target_hostname
```

`-a` specifies an automatic install.

`-v` specifies verbose mode.

`-f` forces Ignite-UX to disregard prior configuration info for that target.

`-i` selects an alternate configuration. If not set, the default is used.

See the *bootsys* (1M) manpage for details on how to select a configuration and to force its use. The default is set in the Ignite-UX server options menu, or can be set manually with the `=TRUE` statement after a `cfg` clause in the `/var/opt/ignite/INDEX` file.

Ignite-UX will contact the target system and extract its hostname, IP address and default gateway. The default configuration is installed. Post install, Ignite-UX will reset the hostname, IP address and gateway to their original values. (remsh access to the target is required. If not available, `bootsys` will prompt the user for the root password on the target.)

This is the quickest way to install a system. The drawback is that you will receive the default config, which may have incomplete networking information unless you are using a previously "saved" configuration, or you specify the defaults in the `/var/opt/ignite/config.local` file as shown later.

Using a "Saved" Configuration

When using Ignite-UX during an install session, you may choose to save the result as a named configuration when finished specifying the configuration for particular target. This will save any changes that you made during the session for use in subsequent sessions. Then either specify the configuration as the default, and/or just use the name you give it to `bootsys` using the `-i` option.

Specifying Defaults in the config.local File

The /var/opt/ignite/config.local file is normally included in every cfg clause in the INDEX file. This provides a convenient location to store default parameters that are the same for all configurations. Typically this will be networking, default software selections, kernel modifications.

It may be easiest to cut and paste information written to the files /var/opt/ignite/clients/*/config by the user interface. However you can do more here than with the Ignite-UX screen. See the *instl_adm* (4) manpage for more details. Below is an example of what a config.local file could look like. The sw_sel's will depend on what you have defined in config files on the server.

```
dns_domain="fc.hp.com"
dns_nameserver[0] = "15.2.72.2"
nis_domain="udl"
wait_for_nis_server=FALSE
root_password="rlW2xSrugUvi2"
timezone="MST7MDT"
ntpdate_server="15.1.48.11"
init sw_sel "Misc_Patches"=TRUE
init sw_sel "B3919DA_AGP"=TRUE
mod_kernel += "maxuprc 100"
mod_kernel += "dbc_max_pct 80"
```

Always run this after making manual edits to verify that the syntax is correct:

```
instl_adm -T
```

See "Setting Install Parameters Dynamically" on page 143 to see how default information may be specified dynamically depending on the target system's configuration.

Setting defaults with instl_adm

Some network parameters need to be known by the target clients when they first boot. bootsys or DHCP/BOOTP can supply the hostname and IP address; however, the netmask and gateway need to be supplied in the RAM filesystem (INSTALLFS). This can done by using the instl_adm command, which has options to set netmask, gateway, Ignite-UX/tftp server, etc. Or you can dump the current settings to a file and edit it, then load the settings back. Just loading Ignite-UX sets some of the parameters.

For example, you may want to set the keyboard language so that it never prompts you for it when booting from Ignite-UX. The file you store using **instl_adm -f** may look like this:

```
# instl_adm defaults:
server="15.2.72.150"
route_gateway[0]="15.2.70.1"
route_destination[0]="default"
netmask[]="255.255.248.0"
# end instl_adm defaults.
kbdlang="PS2_DIN_US_English"
```

Using the per-target client config file

Until now, we have discussed specifying default parameters that all target systems may use. If you would like to specify a specific configuration for an individual target system, you may use the following procedure.

When Ignite-UX begins an install session, it scans the directory `/var/opt/ignite/clients` for a directory matching the *LLA* of the target system. As an example, if the *LLA* of the target is `0x08000992E346`, Ignite-UX looks for a file named `config` in: `/var/opt/ignite/clients/0x08000992E346/config`

Ignite-UX keeps the last configuration installed to the respective system in this file so it can perform a repeat install.

If found, the configuration data in this file is used to overwrite the default values. This file has the highest precedence over all other config files listed in the `INDEX` file.

CAUTION Ignite-UX will write over this file at the end of the install, so you may want to keep an original copy elsewhere.

The easiest way to create the config file is to use one already built by Ignite-UX. If you've previously installed a system (it's best to use one from a similar system to your target,) you can find a config file in the `/var/opt/ignite/clients/`*LLA* directories. Use this as the basis for your new file. Copy it to: `/var/opt/ignite/clients/`*LLA*`/config`

Edit its contents to correspond to your new system.

Example config Ffle

Here is an example config file:

```
cfg "HP-UX B.11.00 archive"=TRUE
_hp_cfg_detail_level="ipvs"
#
# Variable assignments
# init _hp_disk_layout="Whole disk (not LVM) with HFS"
init _hp_pri_swap=68304K
init _hp_root_disk="2/0/1.5.0"
init _hp_sec_swap=0K
init _hp_root_grp_disks=1
init _hp_root_grp_striped="NO"
init_hp_locale="SET_NULL_LOCALE"
init_hp_keyboard="PS2_DIN_US_English"
init _hp_default_final_lan_dev="lan0"
init _hp_boot_dev_path="2/0/1.6.0"
#
# Software Selections
# init sw_sel "golden image"=TRUE
init sw_sel "English"=TRUE
#
# System/Networking Parameters
# hp_custom_sys+={"Current System Parameters", "Original Defaults"}
init _hp_custom_sys="Current System Parameters"
_hp_custom_sys help_text "Final System/Networking Parameters"
(_hp_custom_sys=="Current System Parameters")
{
final system_name="hpfcnjm2"
final ip_addr["lan0"]="15.2.75.14"
final netmask["lan0"]="255.255.248.0"
final dns_domain="fc.hp.com"
final dns_nameserver[0]="15.2.72.254" TIMEZONE="MST7MDT"
is_net_info_temporary=TRUE
}
# end "Current System Parameters"
```

Typically, you would want to change the networking parameters to the correct values. For example:

```
final system_name="system11"
final ip_addr["lan0"]="15.2.75.193"
```

The values specified should be self explanatory, and should be edited to the desired new values. It is also possible to add kernel parameters to this file. See "Setting Install Parameters Dynamically" on page 143 later in this chapter.

You should also update the variable, _hp_cfg_detail_level when adding new types of parameters or they will get lost by the UI or by the file rewrite.

To perform an automatic install with a config file:

Step 1. Determine the *LLA* of the target system, either through the `boot_admin` commands (at bootup) or with the `lanscan` command.

Step 2. Create the following directory (assuming the *LLA* is `0x08000992E346`) and copy in your config file:

```
mkdir /var/opt/ignite/clients/0x08000992E346

cp config /var/opt/ignite/clients/0x08000992E346/config
```

Step 3. Since these files will be accessed using NFS, make sure they have the correct permissions:

```
chown bin:bin /var/opt/ignite/clients/0x08000992E346

chown bin:bin \
/var/opt/ignite/clients/0x08000992E346/config
```

Step 4. Run `bootsys`:

```
bootsys -a -v target_hostname
```

Ignite does not need to be running. Ignite-UX will install the default configuration (or the configuration specified with the `-i` option) and will include the specific changes provided in the config file.

The target system should boot into the Ignite-UX install process and complete the install automatically. Errors will be reported on the client screen and in the `install.log` file.

Monitor the install process via this file:

```
/var/opt/ignite/clients/0x08000992E346/install.log
```

Setting the Local Time Zone

The TZ environment variable governs what time zone the message in the `install.log` contain. The "time zone" config file keyword does not have any effect on the messages that occur during the install, but does determine the time zone setting on the target system (the two can be independently set).

To set the TZ environment variable, it is best to do so in the INSTALLFS file so that it is set as early in the process as possible. However, the first message will still be in EST since it is produced before the config file contents of INSTALLFS are read. The procedure for setting this to MST7DT is:

```
/opt/ignite/bin/instl_adm -d > /tmp/cur_cfg
echo 'env_vars += "TZ=MST7MDT"' >> /tmp/cur_cfg
/opt/ignite/bin/instl_adm -f /tmp/cur_cfg
```

Scheduling Installations

Client installations are easily automated via the cron daemon. For repeated installations, add crontab entries (see *cron* (1M) and *crontab* (1) manpages). For single installations, use the at command. For example, to perform an installation on a target system at 8:00 PM using the at command, as root enter:

```
at 8:00pm
bootsys -a -v target_system (press Ctrl-D)
```

Setting Install Parameters Dynamically

Ignite-UX can make intelligent decisions about install parameters when it runs, based on information it reads from the target system. Instead of forcing static values for example, swap size or kernel parameters, the best values for these can be determined based on the characteristics of the target system.

This can make configurations set up by the system administrator more general purpose and limit the need for multiple, custom configurations to handle minor system differences.

These decisions are specified in a C-like language and grammar unique to Ignite-UX. The variables and syntax are documented in the *instl_adm* (1M) manpage.

Example This example sets the primary swap size of the target system root disk dynamically at install time based on the size of the disk, and on the size of the target system RAM. The algorithm will set swap to 125MB if the disk is large (> 500MB) and if the amount of system RAM is greater than 64MB. If the disk is small, make the swap very small to maximize the amount of space available for HP-UX.

Step 1. Add these lines to the end of the file `/var/opt/ignite/config.local` to be the default for all configurations:

```
# default to very minimal swap of 25MB
# unless the disk is larger than 500 MB
# and we have more than 64MB ram
(disk[_hp_root_disk].size > 500MB & memory > 64MB)
{
   init _hp_pri_swap=125MB
}
else
{
   init _hp_pri_swap=125MB
}
```

You could also put this in a separate file, say, `/var/opt/ignite/data/Rel_B.11.00/custom_cfg`, and add the file name to the `INDEX`.

This could also be added to the `config` file created for automatic installs. Note that if the `_hp_pri_swap` parameter is set later in the order of files searched in the “cfg” definition, this setting will be overwritten. The order the files are evaluated is documented in the *instl_adm* (1M) manpage and in Chapter 3. Also be aware that the `config` file used for automatic installs is overwritten as part of the install process.

Step 2. To force the load of a patch bundle if the target system matches the regular expression `71*`, such as a `710` or `712`, add the following lines to the end of the file:

```
/var/opt/ignite/data/Rel_B.11.00/custom_cfg
# check for H/W model 71x
# and add the Misc_Patches bundle if true
(hardware_model ~ “9000/71*”) {init sw_sel “Misc_Patches” = true}
```

Step 3. Run a previously created post-install script and increase a tunable kernel parameter if we determine our target system is a Model 755. If not, it sets a default value for the kernel parameter:

```
post_config_script += “/var/opt/ignite/scripts/755special”
(HARDWARE_MODEL == “9000/755”) {
   mod_kernel += “maxuprc 300”
} else {mod_kernel += “maxuprc 100”}
```

Step 4. Select an entirely different default configuration based on the size of the system RAM and disk. For this to have effect, it must go into the `INSTALLFS` file by using `instl_adm` as described earlier:

```
# For a system with only one disk and small memory, select
# the “small system configuration”
(num_disks == 1 & memory < 64MB )
{cfg “small system configuration” = true}
```

Step 5. To check the syntax of all configuration files that are listed in the `/var/opt/ignite/INDEX` file, enter:

```
instl_adm -T
```

Step 6. To check the syntax of a file that is not yet in the `INDEX` file, enter:

```
instl_adm -T -f file
```

10 Creating Your Own Install Media

This chapter explains how to create custom installation media to use with Ignite-UX. It's assumed here that you have a basic knowledge of Ignite-UX operations, as explained in the previous chapters.

Why Use Custom Install Media?

You may want to build customized install media ~~if~~:

- You have a large number of systems that are basically identical, and:
  - — The systems do not have network boot capability, or...
  - — The networking will not allow easy or fast access to an Ignite-UX server, or...
  - — The systems are geographically widespread.
- You have HP servers that lack network boot, and so a boot medium is required to contact the Ignite-UX server.
- You want to deliver media to a technician or operator and have the entire install process automated without human intervention or interaction.
- You want a single media that contains all the desired parts of the operating system (HP-UX, applications, patches, diagnostics and local customizations).

Using customized install media also provides both system standardization and customization simultaneously. The standardization comes from using golden system images which contain a base operating system, applications, patches, third-party software and local customizations, already packaged into an archive. The entire system has been tested, verified and tuned before creating the image. This image can be the starting point for all installs to ensure standardization.

The customization comes from using config files to load additional software, change kernel parameters, and run scripts. Software bundles can be:

- Interactively chosen.
- Pre-selected, unconditionally or conditionally.
- Invisible.

There are also parameters that control the environment in which Ignite-UX operates. The most important parameters are `run_ui` and `control_from_server`. When `run_ui` is false, no interaction will occur and the load will proceed according to all the configuration information provided to Ignite-UX. When `control_from_server` is true, an attempt will be made to contact the Ignite-UX server as defined in the configuration information. These modifications are explained in the procedures in this chapter.

Using a custom install media allows you to chose how things work, what you will leave up to the end user, what will happen automatically, and so forth.

Building Example Install Media

The remainder of this chapter describes building custom install media that meets these requirements:

- It will be shipped worldwide so that systems can be installed with a golden image.
- Both a Series 700 workstation and a Series 800 server golden images will be built with the `make_sys_image` command.
- There is a set of applications that are to be chosen interactively by the end user.
- All software will come from the media, and there will be no contact with nor need for an Ignite-UX server during installation. However, you do need an Ignite-UX server to create the media and execute Ignite-UX commands.

Building an Install Tape

This section describes the golden image layout and building an example install tape. We recommend using only 90 metre DDS-1 tapes to make install tapes with Ignite-UX to ensure that the tape will work with any DDS drive. For details on other supported tape formats, see the release notes available from the Ignite-UX Web site.

The Golden Image

Golden system images in these examples were created on Series 700 and Series 800 systems running HP-UX 10.20 using:

```
/opt/ignite/data/scripts/make_sys_image
```

The archives are in tar format and are gzipped. The files are:

```
/var/tmp/archive_700.gz
/var/tmp/archive_800.gz
```

This command has been run on these archives to get disk-space usage information (impacts) so that configuration information can be supplied:

```
/opt/ignite/lbin/archive_impact
```

DDS tape layout

A DDS install tape is constructed logically like this:

Table 10-1 **DDS Install Tape Construction**

LIF	A1/E	D/A2	A3	A4	...

LIF — A bootable tape starts with a Logical Interchange Format (LIF) volume containing all the components required to boot off the tape. It also includes the Ignite-UX toolset and configuration information that controls how Ignite-UX will operate. It includes config file information about the SD depot on the tape (should there be one) and all archives on the media.

A1/E — The next portion is either the first OS Archive (A1) or is Empty (E) if the installation is solely from the software depot.

D/A2 — The next portion is either a serial depot (D) or another OS archive (A2). There can only be one depot on a tape, and it must be the third file on the tape due to a SD restriction.

A3, A4,... — Beyond this, there may be other archives, limited only by the capacity of the tape. If more archives are needed, they can be put on a second medium.

LIF volume content

The make_medialif command is used to create the LIF volume. A typical LIF volume looks like this:

```
volume ISL10 data size 175771 directory size
filename    type   start   size    implement   created
ISL         -12800 16      240     0           98/02/10 14:06:38
AUTO        -12289 256     1       0           98/02/10 14:06:38
INDEX       BIN    264     1       0           98/02/10 14:06:38
CONFIG      BIN    272     58      0           98/02/10 14:06:38
HPUX        -12928 336     800     0           98/02/10 14:06:38
INSTALL     -12290 1136    57503   0           98/02/10 14:06:45
INSTALLFS   -12290 58640   31774   0           98/02/10 14:06:48
INSTCMDS    BIN    90384   9873    0           98/02/10 14:06:51
SYSCMDS     BIN    100264  45901   0           98/02/10 14:07:02
SCRIPTS      BIN    146168   30        0          98/02/10 14:07:02
```

ISL — Initial System Loader. If it is run interactively, it issues a prompt and waits for user interaction. Otherwise it looks for the AUTO file. It is extracted by make_medialif from the default boot file: /opt/ignite/boot/boot_lif

AUTO — Autoexecute file defines the default (possibly automatic) boot behavior.

INDEX — Default INDEX file (it has the same function as /var/opt/ignite/INDEX does on an Ignite-UX server). The file CONFIG is referenced in this file.

CONFIG — Contains all software configuration information. You should begin with the default config file for that release (for example, for the Ignite-UX B.10.20, look in: /opt/ignite/data/Rel_B.10.20/config) Additional config files can be added via the -f option of the make_medialif command. Information in this file will allow complete access to all the archives and depots on the media.

HPUX — HP-UX bootstrap utility. It is also extracted from the default boot file.

INSTALL — 32-bit kernel booted by 32-bit install clients. With a 64-bit kernel, use the make_medialif -o 64 option to create a LIF volume called VINSTALL for V-class systems. For other 64-bit kernels, use the -o 64w option to create WINSTALL files. Use the make_medialif -a option to create all NSTALL and INSTALLFS files.

INSTALLFS — The RAM file system used by install clients. Configuration information stored in the first 8KB of this file is accessible using `instl_adm`. If this is a 64-bit LIF volume, the file is called `VINSTALLFS`. For 64-bit systems, the file is `WINSTALL`.

INSTCMDS — gzip archive of the commands needed for disk layout. These commands run on the install kernel and inside the `INSTALLFS`.

SYSCMDS — gzip archive of commands used to load the software onto the system. There are different archives for each release.

SCRIPTS — gzip archive of all `post_load` and `post_config` scripts that are required. By default when loading a core archive (`load_order` is zero, which means it gets loaded first), the two scripts in `/opt/ignite/data/scripts` called `os_arch_post_l` and `os_arch_post_c` are executed.

Scripts like these are discussed in depth in the *instl_adm* (1M) manpage.

For more information on what happens during system boot and what files do what, see "System Bootup Sequence" on page 162.

Important Config Files

You need to consider two important config file concepts when building archives and bundles to be loaded onto a target system:

- `sw_source` — specifies the access method to either an archive or a depot.
- `sw_sel` — specifies the path of an archive or a bundle in a depot.

For details on these objects, see the *instl_adm* (1M) manpage.

Be sure to pass all user-generated config files through this command to check for syntax errors:

```
instl_adm -T -f cfg_file
```

Accessing a DDS Tape Archive

The best place to start when creating a config file for an archive is to use the template file supplied by Ignite-UX in /opt/ignite/data/examples/. Other files are available for HP-UX 11.0/11i 32- and 64-bit systems. This file can be copied elsewhere, say, to /var/tmp/archive.cfg, and then edited to suit your situation.

Assume that our tape will be used more for installing Series 700 systems than Series 800 systems. Hence, we will put the Series 700 archive on the tape first. In the diagram above, it will be A1. Since there will be a serial depot on the tape, the Series 800 archive will be located at A3.

To modify the config file to access the Series 700 archive, the following attributes need to be changed in /var/tmp/archive.cfg in the sw_source core archive stanza:

Table 10-2

Attribute	Old Value	New Value
source_type	NET	MT
change_media	#change_media=FALSE	change_media=FALSE
nfs_source	nfs_source=*IP:depot*	#nfs_source=*IP:depot*

These changes will modify the source type from network (NET) access (which is either NFS, ftp or remsh) to magnetic tape (MT). Since the archive is going to reside on the same media, change_media is set to false by un-commenting that attribute. To avoid trying to NFS mount that directory, the nfs_source is commented out.

Since the template file already has conditional logic that provides for different Series 700 and Series 800 archives, we will use that to our advantage.

Inside the stanza enabled by HARDWARE_MODEL ~ 9000/7.* the following fields must be changed:

Table 10-3

Attribute	Old Value	New Value
archive_path	B.10.20_700_CDE.gz	1
impacts	/ 27KB	(as reported by archive_impact)

The change in archive_path indicates that there is one EOF mark to skip on the tape and the archive will begin right after that mark. The archive will be the second file on the tape after the LIF volume. The impacts lines must be replaced with whatever was reported by archive_impact for the Series 700 archive.

Inside the same stanza the sw_sel and description strings can be changed to something more descriptive and applicable to your situation. The text inside the double quotes can be changed to whatever you like. They will be visible on the Ignite-UX UI. archive_type must match what was done by make_sys_image. See *instl_adm* (4) for more about archive_type.

Since we have only one Series 700 archive the entire stanza called golden image2 can be deleted. It was included in case you had two different types of archives, for example one for VUE and one for CDE. If more than one archive per architecture is on the media, it is advisable to use an exrequisite attribute between them so only one archive can be selected at one time.

In the stanza for the Series 800 (it is an else clause later in the file) the same sort of changes must be made. However remember that the Series 800 archive is in a different location on the tape. So these attributes need to change:

Table 10-4

Attribute	Old Value	New Value
archive_path	B.10.20_700_CDE.gz	3
impacts	/ 27KB	(as reported by archive_impact)

The change in archive_path indicates that there are three EOF marks to skip on the tape (LIF volume, Series 700 archive, and the serial depot). The Series 800 archive is the fourth file on the tape. The impacts lines must be replaced with whatever was reported by archive_impact for the Series 800 archive.

It is important not to change anything else in the file, unless you are very sure of what you are doing. In particular, it is potentially dangerous to change the sw_category and other sw_source and sw_sel attributes not mentioned above.

Accessing the Serial Depot on a DDS Tape

Assume there is a depot (/var/tmp/depot) that contains all the applications you wish to install on top of the archive. It can be a mixture of Series 700-only applications, Series 800-only applications, and applications that can be loaded on both architectures. Use the make_config command to create config file information for this depot, and the config file is modified to reflect the ultimate destination of the depot.

Step 1. Create config files by entering these commands:

```
make_config -s /var/tmp/depot -a 700 -c
/var/tmp/depot_700_cfg
```

```
make_config -s /var/tmp/depot -a 800 -c
/var/tmp/depot_800_cfg
```

On a tape, the depot must be the third file so there is no need to specify a path to the depot.

Step 2. Change both config files by removing these attribute lines:

```
sd_server = IP_address
sd_depot_dir = /var/tmp/depot
```

Step 3. Change this attribute in both files:

Table 10-5

Attribute	Old Value	New Value
source_type	NET	MT

The deleted information is not needed when accessing a serial depot on a tape. The change to source_type indicates that the depot is located on a tape instead of over the network.

Step 4. Create the Serial Depot. The depot put on a DDS tape is known as a serial depot. It can exist as a regular file, but it cannot be accessed remotely.

To create a serial depot from /var/tmp/depot and store it in /var/tmp/serialdepot, enter:

```
swpackage -s /var/tmp/depot -x target_type=tape \
@ /var/tmp/serialdepot
```

Step 5. Assembling the DDS Tape. Now that all the components of the tape are done, create the LIF volume in /var/tmp/lifvol using the make_medialif command:

```
make_medialif -f /opt/ignite/data/Rel_B.10.20/config \
-f /var/tmp/archive.cfg -f /var/tmp/depot_700_cfg \
-f /var/tmp/depot_800_cfg -l /var/tmp/lifvol
```

This creates the LIF volume that includes all the configuration information, including defaults Ignite-UX provides and information on the archives and depot. For HP-UX 11.0 systems, also use the -a option to include all INSTALL and INSTSALLFS files.

Step 6. Modify INSTALLFS Config. Change configuration information in INSTALLFS. To set run_ui and control_from_server variables using instl_adm to TRUE and FALSE, respectively, based on our scenario:

```
instl_adm -d -F /var/tmp/lifvol > /var/tmp/cfg

vi /var/tmp/cfg        #Add/change the two variables

instl_adm -T -F /var/tmp/lifvol  #Check syntax

instl_adm -d -F /var/tmp/lifvol #Verify changes
```

Step 7. **Make a New Device File.** DDS-1 density is used so that the tape is more readily readable by all DDS tape devices, which are notorious for being finicky at times. To create a device with these characteristics, enter:

```
ioscan -fC tape #get the hardware path
mksf -v -H hardware_path -b DDS1 -n -a
```

You can also create this file using SAM:

1. Click: **Peripheral Devices –> Tape Drives**
2. Select (highlight) the tape drive you want to use: **Actions –> Create Device Files –> Create Custom Device File**
3. Change **DENSITY** to **DDS1**; turn off **Compressed Mode** and **Rewind on Close**
4. Click: **OK**

Step 8. **Create the Install Tape.** Create the tape using a DDS-1 density, no compression, no rewind device file (for example /dev/rmt/c0t3d0DDS1n):

```
mt -t /dev/rmt/c0t3d0DDS1n rew

dd if=/var/tmp/lifvol of=/dev/rmt/c0t3d0DDS1n obs=2k

dd if=/var/tmp/archive_700.gz \
of=/dev/rmt/c0t3d0DDS1n obs=10k

dd if=/var/tmp/serialdepot \
of=/dev/rmt/c0t3d0DDS1n obs=10k

dd if=/var/tmp/archive_800.gz \
of=/dev/rmt/c0t3d0DDS1n obs=10k

mt -t /dev/rmt/c0t3d0DDS1n rew
```

The tape is now ready for installations.

6398
Paula

Building an Install CD-ROM

CD-ROM layout

There are similarities between putting a CD-ROM together and putting a tape together, as explained in the previous pages. One major difference, however, is in disk space usage. You have to create a logical volume (or provide a whole disk) large enough to hold the archives and the depots. This paper will assume that a logical volume is used. You need that much space again to copy the raw logical volume to a regular file. So you probably end up using around three times the disk space consumed by your archives and depots.

A bootable CD-ROM is not a serial device like a tape. It has a file system on it, and it also has a LIF volume that contains the same information as above except for the config files which describe the archives and depots. Access to these objects is somewhat different.

The file system on the CD-ROM can be either HFS or CDFS. You can create an HFS file system using standard HP-UX commands. Various third-party applications are available for a CDFS file system. Note that there is less capacity on a CD-ROM (650 MB) than on a 90 meter DDS-1 tape (2GB).

Step 1. Create the logical volume. Assume that the logical volume that will be used is /dev/vg00/image, and it is mounted at /var/tmp/image. Also assume that an HFS file system will be used. Using HFS and standard HP-UX commands, create the logical volume (assume everything fits in 500 MB):

```
lvcreate -L 500 -n image vg00

newfs -F hfs -f 2048 /dev/vg00/rimage

mkdir -p /var/tmp/image

mount /dev/vg00/image /var/tmp/image
```

For CDFS file systems there are similar commands. Check the software supplier documentation.

Step 2. Access a CD-ROM Archive. The file system in the logical volume will contain both the archives and the depots. Place the archives in the CD-ROM image by copying them into the file system just created:

```
cp /var/tmp/archive_700.gz /var/tmp/image

cp /var/tmp/archive_800.gz /var/tmp/image
```

Step 3. Creating config file information for the archives is similar to what was done for the DDS tape. Start with a new copy of `/opt/ignite/data/examples/core.cfg` in `/var/tmp/archive.cfg`

To modify the config file to access the Series 700 archive, the following attributes need to be changed in `/var/tmp/archive.cfg` in the `sw_source` core archive stanza:

Table 10-6

Attribute	Old Value	New Value
`source_type`	NET	DSK
`change_media`	#change_media=FALSE	change_media=FALSE
`nfs_source`	nfs_source=*IP:depot*	#nfs_source:*IP:depot*

These changes will modify the source type from a network (NET) access to CD-ROM (DSK). The other changes are as described before.

Step 4. Inside the stanza enabled by `HARDWARE_MODEL ~ 9000/7.*` the following fields must be changed:

Table 10-7

Attribute	Old Value	New Value
`archive_path`	`B.10.20_700_CDE.gz`	`archive_700.gz`
`impacts`	/ 27KB	(as reported by archive_impact)

The change in archive_path indicates that the archive will be found in the pseudo-root of the CD-ROM in a file called archive_700.gz . Ignite-UX will prepend the mount point it uses to access the archive. As before, the correct set of impacts lines need to be included.

Step 5. Again you can change the sw_sel and description strings to something more descriptive and applicable to your situation. The text inside the double quotes can be changed to whatever you like. Note that archive_type must match what was done by make_sys_image.

Step 6. Delete the entire stanza called golden image2 again.

Step 7. In the stanza for the Series 800 (it is an else clause later in the file) the same sort of changes must be made. These attributes need to change:

Table 10-8

Attribute	Old Value	New Value
archive_path	B.10.20_700_CDE.gz	archive_800.gz
impacts	/ 27KB	(as reported by archive_impact)

The change in archive_path indicates that the archive will be found in the pseudo-root of the CD-ROM in a file called archive_800.gz. Ignite-UX prepends the mount point it uses to access the archive. As before, the correct set of impacts lines need to be included. It cannot be emphasized enough not to change anything else in the file.

Step 8. **Create and Access the CD-ROM Depot.** Tape is restricted to a single depot. That restriction does not apply to a CD-ROM. However, we will use a single depot for simplicity sake. Create the depot using swcopy to a target in the logical volume:

```
swcopy -s /var/tmp/depot \* @ /var/tmp/image/depot
```

Step 9. Once again, use make_config to create the start of the config files for the depot:

```
make_config -s /var/tmp/depot -a 700 -c
/var/tmp/depot_700_cfg
```

```
make_config -s /var/tmp/depot -a 800 -c
/var/tmp/depot_800_cfg
```

Step 10. **Edit config Files.** Since the SD server is the system that is being installed, remove this attribute. Change both config files by removing this attribute line:

```
sd_server=IP_address
```

Step 11. **Change these attributes in both files:**

Table 10-9

Attribute	Old Value	New Value
source_type	NET	DSK
sd_depot_dir	var/tmp/depot	depot

The change to source_type indicates that the depot is located on a CD-ROM instead of over the network. The change in sd_depot_dir indicates that the depot will be found in the pseudo-root of the CD-ROM in a depot called depot. Ignite-UX prepends the mount point it uses to access the depot.

Step 12. **Assemble the CD-ROM.** The raw file system just created must be copied into a regular file so it can be written to the CD:

```
umount /var/tmp/image

dd if=/dev/vg00/rimage of=/var/tmp/fs_image bs=1024k
```

Step 13. **Create the LIF Volume.** Now that most of the components of the CD-ROM are complete, use make_medialif to create the LIF volume:

```
make_medialif -f /opt/ignite/data/Rel_B.10.20/config \
-f /var/tmp/archive.cfg -f /var/tmp/depot_700_cfg \
-f /var/tmp/depot_800_cfg -l /var/tmp/lifvol
```

This creates the LIF volume that includes all the configuration information. It includes the defaults Ignite-UX provides and provides the access to the archives and the depot.

Step 14. Modify INSTALLFS Config. Change configuration information in INSTALLFS. To set run_ui and control_from_server variables using instl_adm to TRUE and FALSE, respectively, based on our scenario:

```
instl_adm -d -F /var/tmp/lifvol > /var/tmp/cfg

vi /var/tmp/cfg    #Add/change the two variables

instl_adm -T -F /var/tmp/lifvol    #Check syntax

instl_adm -d -F /var/tmp/lifvol    #Verify changes
```

Step 15. These two objects (the raw file system and the LIF volume) must be combined using instl_combine. The result is a single file with the LIF volume wrapped around the file system, which can then be written to the CD:

```
/opt/ignite/lbin/instl_combine -F /var/tmp/lifvol \
-C /var/tmp/fs_image
```

Step 16. Complete the CD config. Using your CD-ROM writer software, copy /var/tmp/fs_image to the CD.

The CD-ROM is now ready for installations. You can test the image out before burning a CD by copying it to an unused raw disk and rebooting the system off that disk.

Media from make_tape_recovery

There are many similarities between a tape produced by make_tape_recovery and one constructed by the method described here. In fact, make_tape_recovery performs many of the same steps. But there are some important differences as well. The primary purpose of a recovery tape is to restore enough of a system to get it going following some catastrophe, so the rest of the system can be recovered from backups.

Additional Archives and Depots Media

If there is insufficient space on either a tape or a CD to hold all the archives and depots, it is possible to put them onto separate media. In this case, the config file describing these archives or depots would have change_media set to true. Ignite-UX would prompt the user for the new medium. If this is a CD, the instl_combine step is needed only for the first CD.

E 6392 Paula

System Bootup Sequence

This sequence of events occurs when an HP computer system boots up:

Step 1. The firmware determines from which device to boot via either user input or primary path.

Step 2. The firmware looks for a LIF header on that device, and if it finds it, it looks in the LIF header for where the ISL starts.

Step 3. The firmware loads the ISL into memory from the boot device and executes it. It passes a flag to it that indicates whether to run interactively or to autoboot.

Step 4. If the ISL is interactive then it gives the `ISL>` prompt and waits for user input before proceeding.

Step 5. If the ISL is not interactive, then it looks for the `AUTO` file on the boot device to determine what to run next.

Step 6. The `AUTO` file or user input usually supplies the `hpux` *args* command. This tells ISL to load the program `HPUX` from the LIF header on the boot device and to run it with the given arguments.

Step 7. The hpux program (also known as the secondary loader) figures out what HP-UX kernel to load, and what arguments to pass to it (like init state).

Step 8. `hpux` loads the kernel and starts running it.

Step 9. For the INSTALL kernel, the kernel looks at its name and realizes that it fits the pattern `*INSTALL` and then loads the matching `*INSTALLFS` file from the boot device.

In all these cases the firmware (Processor Dependent Code, or PDC) API services are used when accessing the boot device.

11 System Recovery

This chapter describes important system recovery tools available with Ignite-UX:

- Creating a Bootable Recovery Tape.
- Duplicating make_tape_recovery Tapes.
- Creating a Recovery Archive via the Network and Tape.
- Archive Creation Steps.
- Verifying Archive Results.
- Retaining “Known-good” Archives.
- Making config File Additions.
- Selecting File Systems During Recovery.
- Tape Recovery with make_net_recovery.
- Tape Recovery with No Tape Boot Support
- Notes on Cloning Systems.
- Expert Recovery Using the Core Media.
- System Recovery Questions and Answers.

NOTE

The `make_tape_recovery` tool replaces `make_recovery` for creating recovery tapes, beginning with Ignite-UX A/B 3.2, March 2001. With the `make_tape_recovery` command, you can make recovery archives on local and remote systems, as explained in this chapter. For more details, see the *make_tape_recovery* (1M) manpage.

Overview

HP-UX provides two recovery methods as part of the standard product: system recovery and expert recovery. The method you use depends on the situation.

System Recovery via Network and Tape

The system recovery tools available with Ignite-UX allow you to quickly recover from a failed disk (root disk or disk in the root volume group). The failure can be either a hardware failure or a catastrophic software failure.

System recovery requires some work *before* a problem occurs. On a regular basis, you need to run the appropriate tool on each of your systems: use the `make_net_recovery` command to create an archive on another system or the `make_tape_recovery` to create an archive on tape.

The `make_tape_recovery` and `make_net_recovery` commands both create a bootable recovery (install) archive which is customized for your machine. The archive contains your system's configuration information (disk layout, etc.) and files on your root disk or root volume group. You can exert some control over which files are saved as part of the archive.

Once you have a recovery archive on tape or another system, recovering a failed system is easy:

1. If a disk failed, replace it.
2. Boot from your recovery tape or system.
3. Wait for the recovery to complete.
4. Once the system comes back up, recover the latest copies of files from the last system backup.

Expert Recovery

Expert recovery, formerly called Support Media Recovery, allows you to recover a slightly damaged root disk or root volume group. With this method, you repair the boot/root disk and root volume group from the network or HP-UX Core media. Once the recovery system has been booted, you can:

- Put a known, good kernel in place.
- Fix the LIF volume on the disk.
- Copy essential files and commands into place.

Expert recovery does not require that you do any preparation before you use it. The media used is supplied by HP; it is not customized to your site. In addition to the media, you can also boot from your Ignite-UX server. However, this also means that any customization you have are not reflected in the files you recover via expert recovery. Depending on the failure cause, expert recovery gives you enough capabilities to get your system back up again. At that point, you need to use your normal restore tool to recover your system to the state it was in before the problem occurred. Expert recovery is not useful to recover from hardware failures.

System Recovery Tools

Comparing Features

The make_net_recovery and make_tape_recovery tools share many features in common with few differences that exist, mainly due to the different media that are used and ways of handling them. Both system recovery tools share the same basic archive creation options, data structures, archive file content, and installation dialogues.

To determine which system recovery tool is best suited for your needs, consider the following:

Use make_tape_recovery if:

- Managing a single or limited number of systems locally
- Cloning a "like system"
- Systems are not networked
- Suitable tape drive exists.

6388
Paula

- Tape media is needed for an off-site recovery system

Use `make_net_recovery` if :

- Managing central, networked systems
- Cloning a "like system"
- Avoid tape issues (media cost and handling, multi-tape archives, etc.)
- Suitable disk space for archive storage
- Performing unattended backups without tape handling

The following table summarizes and compares some of the features of the `make_tape_recovery` and `make_net_recovery` tools:

Table 11-1 **Comparing System Recovery Tool Features**

Feature	`make_tape_recovery`	`make_net_recovery`
Minimum hardware configuration	Stand-alone system; local tape drive	Two networked systems; sufficient disk space to hold archive
Archive Creation Interface	Client command line; Server GUI; Client TUI	Server GUI; Client command line; Client TUI
Archive	Self contained image; written to the client's tape drive	Requires an Ignite-UX server to install; written to NFS mounted file system

Archive Contents

The `make_net_recovery` and `make_tape_recovery` commands allow you to view and control archive contents:

- The list of essential files to be included in the archive is available as a simple text file: `/opt/ignite/recovery/mnr_essentials`. This file allows you to see what files and directories are included by default in the archive.
- You can specify what additional volume groups, directories, and files you want included, and what directories and files you want excluded. This is done using simple syntax in the client-specific content file, `/var/opt/ignite/clients/LLA/recovery/archive_content` or

using command line options. You are not restricted to one or two volume groups. You can create a complete multi-volume group file system archive if you want.

- You can use the user interface to find out which volume groups and/or disks will be untouched, which will be partially restored, and which will be restored in full if the archive is used, based on the specifications in the `mnr_essentials` file and the `archive_content` file.
- You can also use the user interface to edit the `archive_content` file and dynamically see the changes in the volume groups and disks that are affected.
- The policies for user-specified content are documented in "Archive Configuration Policies" on page 175.

`make_tape_recovery` creates a bootable tape that can be used to restore a system via the system's tape drive. `make_tape_recovery` is subject to the requirements and limitations inherent with tape media:

- A tape drive must be available on each system to be archived.
- If you want to save the previous good archives before creating new ones, you need to remove the old tapes and insert different tapes on each system.
- If an archive exceeds the capacity of a tape, you need to swap tapes for both creation and extraction.
- If you want to make sure that the newly created tapes are good, you need to check the log files on every system.
- Tape drives are more error-prone than a local network.

Dependency on Ignite-UX Server for Recovery

make_tape_recovery

The tape created by `make_tape_recovery` is completely self-contained and does not require an Ignite-UX server. The `make_tape_recovery` archive contains a specially prepared LIF volume. The config file in the LIF volume is the configuration file for the archive. The `INDEX` file in the LIF volume specifies the recovery configuration as the default for the system. The `INSTALLFS` in the LIF volume contains additional configuration information so no user interaction will take place. Additional files needed for booting and installing are copied from

6386
Paula

/opt/ignite/boot and /opt/ignite/data to the LIF volume, so that everything the system needs to recover is there. You could use your make_tape_recovery tape even if you removed your Ignite-UX server.

make_net_recovery The archives created by make_net_recovery are designed to work with an Ignite-UX server; you could not remove your server and still use your recovery archive.

Creating a Bootable Recovery Tape

IMPORTANT

copyutil is a diagnostic tool for HP-UX 10.*x* or later, and should not be used for system recovery. Instead, use one of the tools described in this chapter.

Ignite-UX's make_tape_recovery command can create a system recovery tape. This tape can be used to boot and recover a system which has become unbootable due to corruption of the root disk or volume group. A system can be booted and installed from the tape without user intervention for configuration, customization, software selection, hostname, or IP address.

NOTE

A bootable recovery tape can also be created from the Ignite-UX server. However, the client must have a local tape drive.

The make_tape_recovery tool creates a system recovery archive and stores the archive on a local tape. make_tape_recovery is capable of creating system recovery tapes for tape devices, with the ability to span multiple tapes. The archive created by make_tape_recovery is specific to the system it was created for and its identity includes hostname, ip_address, networking information, etc. In the event of a root disk failure, the recovery archive can be installed via tape to restore the system.

The contents of the system recovery archive will always include all files and directories which are considered essential to bringing up a functional system. This **essential** list is pre-defined by make_tape_recovery and is located in the following file: /opt/ignite/recovery/mnr_essentials. By running make_tape_recovery in interactive mode, the directories and files which make up the essential list can be displayed. In addition to the essential list, data can be included in the archive on a disk/volume group, file, or directory basis. Non- essential files and directories can also be excluded.

NOTE

It is preferable to use the Ignite-UX GUI menu command on the Ignite-UX server when running an interactive make_tape_recovery session. Running it from Ignite-UX causes any additional server configuration of NFS mounts to be performed. It also provides a better progress report and an easier to use interface.

Logging

On a server, progress and errors are logged to:

/var/opt/ignite/clients/<*LLA*>/recovery/<*datetime*>/recovery.log

On a local system, progress and errors are logged to:

/var/opt/ignite/recovery/<*datetime*>/recovery.log

Task: Recover a minimal OS

Preform these operations as root.

To create a minimal operating system recovery tape at /dev/rmt/0mn, containing only the OS elements required to boot the system, perform the following steps:

Step 1. Load a writable tape in the default tape drive for your system.

Step 2. Enter: **make_tape_recovery**

A tape will be created without further interaction.

System recovery from this tape would involve booting from the tape to recover the minimum Core OS. Then you would follow up with data recovery of all user files newer than those restored from the recovery tape.

Task: Create a system recovery archive of entire root disk volume

To create a system recovery tape at the default device /dev/rmt/0m, and that includes the entire root disk in the archive, perform the following steps:

Step 1. Load a writable tape in the default tape device for your system.

Step 2. Enter the appropriate command:

```
make_tape_recovery -x inc_entire = vg00
```

A tape will be created without further interaction.

Task: Create a system recovery archive tape with the -A option

To create a system, you can create a system recovery tape as follows:

Step 1. Load a writable tape in the default tape device for your system.

Step 2. Enter: `make_tape_recovery -A`

A tape will be created without further interaction. You can boot this tape on your new system.

Task: Install a system recovery from an archive tape

To install a system recovery from an archive tape:

Step 1. Mount the system recovery tape on the tape drive.

Step 2. Boot the system.

Step 3. Interrupt the boot sequence to redirect it to the tape drive by pressing **Esc**.

Step 4. Cancel the non-interactive installation by pressing any key when given the opportunity.

Step 5. Allow the install process to complete.

For more information on creating recovery tapes, see the *make_tape_recovery* (1M) manpage.

Duplicating make_tape_recovery Tapes

A tape created with `make_tape_recovery` contains two tape "files": a 2KB LIF file and a 10 KB tar archive. If you have two tape drives on a system, you can easily duplicate the tapes using two `dd` commands with a no-rewind-on-close device file for the first command. For example:

```
dd if=/dev/rmt/0mn of=/dev/rmt/1mn bs=2k
dd if=/dev/rmt/0m of=/dev/rmt/1m bs=10k
```

If you only have one tape drive, and have enough disk space to hold the contents of both tape files, use something like this:

```
dd if=/dev/rmt/0mn of=/var/tmp/f1 bs=2k
dd if=/dev/rmt/0m of=/var/tmp/f2 bs=10k
```

(Insert blank tape now)

```
dd if=/var/tmp/f1 of=/dev/rmt/0mn bs=2k
dd if=/var/tmp/f2 of=/dev/rmt/0m bs=10k
```

Also see the *copy_boot_tape* (1M) manpage.

Creating a Recovery Archive via the Network and Tape

Ignite-UX A.2.0, B.2.0 and later versions allow you to create recovery archives via the network onto the Ignite-UX server system, or any other specified system. You can either use the Ignite-UX `/opt/ignite/bin/ignite` or run `/opt/ignite/bin/make_net_recovery` on a client system. Use Ignite-UX to recover specified systems on the net. Systems can be recovered across subnets from a boot tape using `make_boot_tape`, local boot server or the `bootsys` tool from an Ignite-UX server.

The `make_net_recovery` tool creates a system recovery archive and stores the archive on the network. The archive created by `make_net_recovery` is specific to the system it was created for and its identity includes hostname, ip_address, networking information, etc. In the event of a root disk failure, the recovery archive can be installed via Ignite-UX to restore the system.

The contents of the system recovery archive will always include all files and directories which are considered essential to bringing up a functional system. This essential list is pre-defined by `make_net_recovery`. By running `make_net_recovery` in interactive mode, the directories and files which make up the essential list can be displayed. In addition to the essential list, data can be included in the archive on a disk/volume group, file, or directory basis. Non- essential files and directories can also be excluded.

Networking features

Two NFS mount points are established on the client by `make_net_recovery`. The `/var/opt/ignite/clients` directory on the Ignite-UX server is mounted to the client system to store configuration files which describe the client configuration and location of the recovery archive. The second mount point is made to the *`archive_server:archive_dir`* (see the `-a` option) and is used to store the recovery archive of the client system. After successful or unsuccessful completion of the system recovery archive, the NFS mount points are un-mounted.

The NFS mount for the archive directory may be exported on a per-client bases. A separate archive directory is used for each client. This allows you to NFS export each directory only to the individual client owning the archive, which provides security.

If the client system does not have the most recent versions of Ignite-UX tools, the Ignite-UX GUI uses `swinstall` to install the "recovery package" which includes all necessary files to perform the recovery.

Create a Recovery Archive from the Ignite-UX Server

To create a system recovery archive from an Ignite-UX server:

Step 1. On your host system, allow the Ignite-UX server access to your to display by adding the Ignite-UX server hostname to your xhost list:

```
xhost + Ignite-UX_server_hostname
```

Step 2. Set the DISPLAY variable to your local host system, if necessary. For example:

```
export DISPLAY=Elvis:0
```

Step 3. On the Ignite-UX server, as root run:

```
/opt/ignite/bin/ignite
```

Step 4. Select: **Actions –> Add New Client for Recovery** You will need to respond to a dialogue to identify the system.

Step 5. Click the client icon when its appears on the Ignite-UX screen.

Step 6. Select: **Actions –> Create Network Recovery Archive.** You may be prompted for the root password for the targetsystem.

The network recovery tools needed on the client will automatically be installed.

After some information screens, you will see an Include/Exclude selection screen. To view the essential files, click the **Show** button. Essential files cannot be excluded, but you can customize the archive by specifying additional volumes, directories, or files. In case an item is duplicated as both Include and Exclude, the Exclude category dominates.

Archive Configuration Policies

When specifying archive content for both make_net_recovery and make_tape_recovery, either via the Ignite-UX GUI or the command line, the following rules apply:

- No essential file or directory can be excluded.
- Files and directories inside an included directory will be included recursively.
- If a symbolic link to a file or directory is included, only the link will be included in the archive, not the actual file or directory, unless it, too, is included. A warning will be given when the item itself is a symbolic link.
- If a directory is included which contains symbolic links to other files or directories, the symbolic links will be included but not the referenced files or directories, unless they, too, are included. No warnings are given regarding these links.
- If a directory contains local mount points, the files and directories under the local mount points will not be included, by default. This policy can be waived by specifying the option inc_cross (include directory and cross-mount points), in the selection interface or command line.
- In case of conflicting entries in the selections, Exclusions take precedence over Inclusions.

IMPORTANT If there are mount points below /etc, make_net | tape_recovery will not restore these files until the recovery generates errors. The recovery does not fail, but the mount points under /etc are missing.

More Examples

The follow examples apply for system recovery using either `make_net_recovery` or `make_tape_recovery`:

Create recovery from the client

This command creates a system recovery archive from the client, using settings from the last invocation of Ignite-UX, and using the options file on the Ignite-UX server (`myserver`) in the default location, */var/opt/ignite/clients/0xLLA/recovery/*:

```
make_net_recovery -s myserver
```

Create recovery from the client that includes volume group files

To create a system recovery archive from the client that includes files from all file systems in the `vg00` volume group, enter:

```
make_net_recovery -s myserver -x inc_entire=vg00
```

Create recovery archive file to replace mnr_essentials

To create a system recovery archive with all the files/directories on the disk(s)/volume group(s) containing the files specified by the default essentials file list `/opt/ignite/recovery/mnr_essentials` or the user defined version of this file, that replaces this file, `/var/opt/ignite/recovery/mnr_essentials`, enter:

```
make_net_recovery -s myserver -A
```

Preview system recovery

To preview the creation of the system recovery archive enter:

```
make_net_recovery -p
```

Large File Support

Specific support for large files is needed if archives greater than 2GB are to be created. This requires ensuring that both the file system and the NFS mount on the archive server will support large files.

The `fsadm` command can be used to determine whether large files are currently supported on a specific file system. The *fsadm* (1M) manpage has an example of how to change the file system to support large files. If you use `fsadm` to convert a file system, re-run **`exportfs -a`**, if it is already exported, in order for clients to be affected by the change.

To support NFS mount and network data transfer of large files, you will need to have NFS PV3 installed on both the client and server. If the client or server is running HP-UX 10.20, the Networking ACE patch (containing the NFS PV3 software) should be installed and updated with a patch cited in the Ignite-UX Release Notes. HP-UX 11.0 and later versions come with PV3 by default.

The Ignite-UX Release Notes (`/opt/ignite/share/doc/release_note`) identifies which patches are required for NFS support of archives greater than 2GB for HP-UX 10.20, 11.0 and later.

Recovering via the Network for PA Clients

To recover a failed disk or volume group using the system recovery archive:

Step 1. Boot the failed system using one of these ways (see "Booting Client Systems from the Network" on page 67):

- Using Ignite-UX after booting with: **`boot lan install`**
- Booting from an Ignite-UX server, using `bootsys` if the client OS is running.
- Booting the failed client locally by using a boot tape previously created with `make_boot_tape`.

Step 2. Do not interact with ISL.

Step 3. From the main menu, select **Install HP-UX**
At the client:

1. Respond to Network configuration dialogue screen.
2. Respond to the UI display options (run at Server or at Client).
3. If working from the Ignite-UX server, select the client icon for the system to be recovered.

Step 4. Select **Install/New Install**

Step 5. Select the recovery configuration to use.

Recovering via the Network for IA Clients

To recover a failed disk or volume group using the system recovery archive:

Step 1. From the EFI Boot Manager menu, you will see a prompt to select a boot option. Select **`Boot option maintenance menu`**.

```
EFI Boot Manager ver 1.10 [14.54]  Firmware ver 0.0 [4209]

Please select a boot option

    EFI Shell [Built-in]
    Boot option maintenance menu
    Security/Password Menu (*** Prototype ***)

Use up and down-arrows to change option(s).
Use Enter to select an option
```

Step 2. The Main Menu appears and prompts you to choose an operation. Select **`Add a Boot Option`**.

```
EFI Boot Maintenance Manager ver 1.10 [14.54]

Main Menu. Select an Operation

        Boot from a File
        Add a Boot Option
        Delete Boot Option(s)
        Change Boot Order

        Manage BootNext setting
        Set Auto Boot TimeOut

        Select Active Console Output Devices
        Select Active Console Input Devices
        Select Active Standard Error Devices

        Cold Reset
        Exit
```

Step 3. The following menu displays. Select an appropriate network card for network boot. For example, look for entries with a MAC followed by the Mac/*LLA* address of the LAN card.

```
EFI Boot Maintenance Manager ver 1.10 [14.54]

Add a Boot Option.  Select a Volume

    Removable Media Boot
[Acpi(HWP0002,0)/Pci(2|0)/Ata(Primary,Maste
    Load File [EFI Shell [Built-in]]
    Load File [Acpi(HWP0002,0)/Pci(3|0)/Mac(00306E1E4ED4)]
    Load File [Acpi(HWP0002,100)/Pci(2|0)/Mac(00306E1E3ED6)]
    Exit
```

Step 4. Enter an appropriate boot option name at the message prompt. For this example, new boot options are named LAN1 and LAN2.

Step 5. Exit to the main menu. The new boot option will now appear in the EFI Boot Manager main menu.

```
EFI Boot Manager ver 1.10 [14.54]  Firmware ver 0.0 [4209]

Please select a boot option

    SCSI2-HPUX
    EFI Shell [Built-in]
    LAN2
    LAN1
    Boot option maintenance menu
    Security/Password Menu (*** Prototype ***)

Use up and down-arrows to change option(s).
Use Enter to select an option
```

Step 6. Select the new boot option you created. The following is an example of a successful boot using the new boot option.

```
Loading.: LAN1
Running LoadFile()

CLIENT IP: 15.1.52.128  MASK: 255.255.248.  DHCP IP: 15.1.53.37
GATEWAY IP: 15.1.48.1
Running LoadFile()

Starting: LAN1

@(#) HP-UX IA64 Network Bootstrap Program Revision 1.0
Downloading HPUX bootloader
```

6374
Paula

```
Starting HPUX bootloader
Downloading file fpswa.efi  (371200 bytes)

(c) Copyright 1990-2001, Hewlett Packard Company.
All rights reserved

HP-UX Boot Loader for IA64  Revision 1.671

Booting from Lan
Downloading file AUTO   (528 bytes)
Press Any Key to interrupt Autoboot
AUTO ==> boot IINSTALL
Seconds left till autoboot -   0
AUTOBOOTING...
```

Step 7. From the main menu, select **Install HP-UX**
At the client:

1. Respond to Network configuration dialogue screen.
2. Respond to the UI display options (run at Server or at Client).
3. If working from the Ignite-UX server, select the client icon for the system to be recovered.

Step 8. Select **Install/New Install**

Step 9. Select the recovery configuration to use.

Create a Bootable Archive Tape via the Network

This section explains how to create a self-contained recovery tape for a recovery configuration already stored on an Ignite-UX server via network system recovery. See the *make_net_recovery* (4) manpage for more details. It is important that the archive fit onto a single tape.

These instructions assume that:

- The hostname of the machine the archive was created for is sys1.
- The archive was created at “2001-03-12,09:00”.
- The archive will fit onto a single tape.

Step 1. Build the LIF file. The LIF file will contain the Ignite-UX tools and environment, the config files produced for the recovery archive, and the scripts used during recovery.

1. Use `make_medialif` to build the LIF file:

```
cd
/var/opt/ignite/clients/sys1/recovery/2001-03-12,09:00

make_medialif -f system_cfg -fcontrol_cfg -f archive_cfg\
-C "2001-03-12,09:00 sys1 recovery image" \
-l /var/tmp/my_lif -a -r os_rev
```

2. Modify the LIF file for use on the tape:

```
instl_adm -d -F /var/tmp/my_lif > /var/tmp/cfg
```

3. Add these lines to the end of the `/var/tmp/cfg` file:

```
control_from_server=FALSE

run_ui=TRUE
```

OR, if you just want the recovery to proceed without any interaction, make:

```
run_ui = FALSE
```

and specify to allow warnings as shown here:

```
env_vars += "INST_ALLOW_WARNINGS=10"
```

4. Enter:

```
instl_adm -F /var/tmp/my_lif -f /var/tmp/cfg
```

Step 2. Create the Tape. To write the LIF and archive to a tape:

1. Determine which tape device file you can use to write the tape. The device file must match the tape drive type you will use when actually recovering the system. Also, the tape device file must be the no-rewind type. For the rest of this example, assume that `/dev/rmt/c1t0d0DDS1n` is a no-rewind DDS-1/no compression device file.

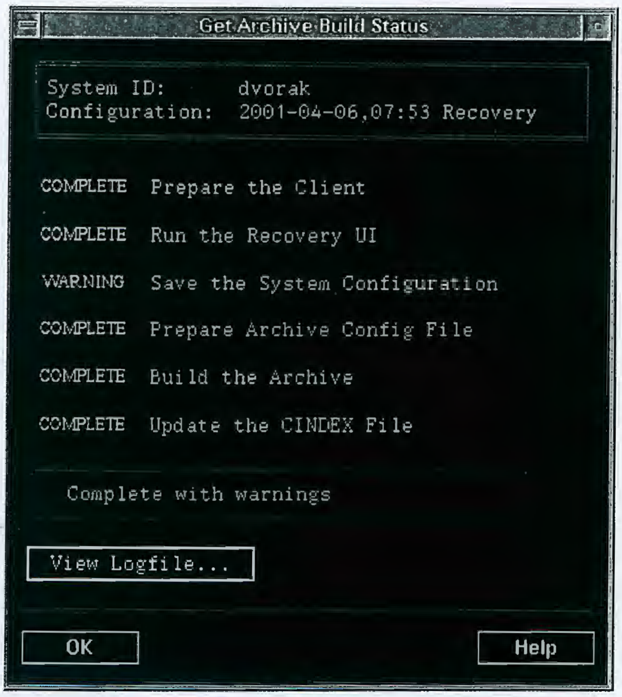
2. Rewind the tape, write out the LIF and archive, and rewind again:

```
mt -t /dev/rmt/c1t0d0DDS1n rew

dd if=/var/tmp/my_lif of=/dev/rmt/c1t0d0DDS1n obs=2k

dd if=/var/opt/ignite/recovery/archives/sys1/2001-03-12,
09:00 \ of=/dev/rmt/c1t0d0DDS1n obs=10k

mt -t /dev/rmt/c1t0d0DDS1n rew
```

In this example, the archive is retrieved from the standard location on the Ignite-UX server for this host. If you have chosen to put the archive elsewhere, refer to that location instead.

Archive Creation Steps

Ignite shows the steps as an archive is being created with `make_net_recovery`:



```
System ID:      dvorak
Configuration:  2001-04-06,07:53 Recovery

COMPLETE   Prepare the Client
COMPLETE   Run the Recovery UI
WARNING    Save the System Configuration
COMPLETE   Prepare Archive Config File
COMPLETE   Build the Archive
COMPLETE   Update the CINDEX File

  Complete with warnings
```

Step 1. Prepare the client. `make_net_recovery's` primary tasks are to check that the recovery tools installed on the client are compatible with the versions on the Ignite-UX server, and to create the necessary directories and files. If the client was not previously installed using the Ignite-UX server, `make_net_recovery` creates a new directory for the client in `/var/opt/ignite/clients` on the server.

`make_net_recovery` also generates a timestamp for naming the archive, the configuration, and the configuration directory. The directory containing the configuration files for the archive will be something like:

`/var/opt/ignite/clients/`*`LLA`*`/recovery/2001-03-09,00:27`

The corresponding archive will be:

```
/var/opt/ignite/recovery/archives/client/2001-03-09,00:27
```

The timestamp is important for coordinating configuration files and archives, and for ongoing archive management.

Here's an overview of files located in the client's directory for network recovery (for a local tape the path would be /var/opt/ignite/recovery):

```
/var/opt/ignite/clients/<LLA>
        install.log
        CINDEX
        Client_status
        recovery/
                archive_content
                defaults
                latest
                2001-02-09,00:27/
                        archive_content
                        system_cfg
                        archive_cfg
                        config_cfg
                        recovery.log
                        flist
                        manifest
                2001-03-09,00:27/
                        archive_content
                        system_cfg
                        archive_cfg
                        config_cfg
                        recovery.log
                        flist
                        manifest
```

Step 2. Run the recovery Interface. If `-i` is specified on the command line, the Recovery user interface is run next. The interface enables users to set or change the following default values for the archive:

- Long description of the archive. This description may be used to add identifying information that can help to distinguish archives when the timestamp is not sufficient. This information is shown by clicking **Description** on the **Basic** tab during installation configuration.

- Maximum number of archives to keep. When the number of archives in the destination directory reaches this maximum, `make_net_recovery` removes the oldest archive. It uses the timestamp in the name of the archive to determine which one to remove.

- Destination host for the archive.

- Destination directory for the archive.

The user interface also gives users the opportunity to review and edit the `archive_content` file as mentioned above. When the user exits the recovery user interface, the default values that the user entered are written to:

`/var/opt/ignite/clients/`*`LLA`*`/recovery/defaults`

The archive content is written to:

`/var/opt/ignite/clients/`*`LLA`*`/recovery/archive_content`

Step 3. Save the system configuration. For all volume groups, even ones that are not included in the archive, `make_net_recovery` now backs up volume group configuration information and stores in the `system_cfg` file. It also obtains map files for volume groups that are not part of the archive using `vgexport`. The volume group configuration files and the map files generated at this stage are stored in `/etc/lvmconf`. This directory is included by the list of essential files, so the lvm files are included in the archive.

After the volume group information is saved, `make_net_recovery` creates the `control_cfg` file. This file includes the `post_config_cmds` to import all volume groups that were not included in the archive and to activate all volume groups that were imported. It also includes control flags, such as `recovery_mode=true`, to guide the behavior of Ignite-UX during recovery.

Step 4. Prepare the config file. Once the archive is created, `make_net_recovery` calls `make_arch_config` to create the `archive_cfg` file to reference it. `make_arch_config` uses `archive_impact` to calculate the file system impacts for the archive, and includes these in the `sw_sel` stanza it writes.

Step 5. Build the archive. make_net_recovery calls make_sys_image to create the archive. make_sys_image passes a pre-built flist to calculate the total disk space currently used by all the files to be included in the archive. It uses this information with a compression ratio to estimate the final size of the archive. If the destination directory has sufficient free disk space for the archive, make_sys_image creates the archive using pax.

Step 6. Update the CINDEX file. make_net_recovery uses manage_index to update the /var/opt/ignite/clients/*LLA*/CINDEX file for the client. This file contains a list of all the recovery cfgs available for the client. An entry for the most recently created archive looks something like this:

```
cfg "1999-03-10,00:27 Recovery" {
   description "This cfg is a pure mnr_essentials recovery
   archive."
   "recovery/1999-03-10,00:27/system_cfg"
   "recovery/1999-03-10,00:27/control_cfg"
   "recovery/1999-03-10,00:27/archive_cfg"
}=TRUE
```

Verifying Archive Contents

What files will be archived?

To list the files and directories that will be included in a make_net_recovery archive, enter:

```
/opt/ignite/lbin/list_expander -l -f input_file
```

You can examine the list of files that will be re-created during an installation from a make_net_recovery configuration, by viewing the /var/opt/ignite/clients/cca/recovery/fhist file. For example:

```
pg /var/opt/ignite/clients/cca/recovery/fhist
```

If make_tape_recovery was used, the list of recovery files resides in /var/opt/ignite/recovery/latest/fhist and can be viewed in the same manner as the above example.

What disks or volume groups will be recovered?

To list disks or volume groups that will be re-created during an installation from a make_net_recovery configuration, enter this from the client:

```
/opt/ignite/lbin/list_expander -d -f input_file
```

where: *input_file* is a file specifying what is to be archived. See the *make_net_recovery* (4) manpage for details on the format of the *input_file*. make_net_recovery can take input from an input file, no input, or input from the command line with the -x option. list_expander can take input from an input file, or no input, but does not have an x option like make_net_recovery does, so to see the result of using x options, put them in a file and pass list_expander the file name.

If you used the Ignite-UX to specify what is to be included in the archive, then the input file can be found on the server in:

/var/opt/ignite/clients/*client*/recovery/archive_content

You can copy this file from the server to the client, then run list_expander against that file itself.

Omitting -f *input_file* causes list_expander to use only the essential files as input. This will show what disks or volume groups will get re-created for the minimal archive. Here's an example output:

```
In?     dsk/vg   name         minor#  Associated disks
0       d         /dev/dsk/c0t3d0
1       v        /dev/vg00      0x00     /dev/dsk/c0t6d0
                                          /dev/dsk/c0t4d0
0       v         /dev/vg01      0x01     /dev/dsk/c0t1d0
0       v        /dev/vg02      0x02    /dev/dsk/c0t2d0
```

The dsk/vg column shows that the system has one whole disk (d) and three volume groups (v). The next column gives the names of the disks and volume groups. The In? column shows, for each disk or volume group, if it will be:

2 = included in full (INC_ENTIRE dsk/vg specified),

1 = included in part (some files included, some not), or

0 = not included at all (no files from this dsk/vg are included).

0 means the disk or volume group will *not* be touched. 1 or 2 means that the disk or volume group *will* be re-created, and files from the archive will be restored during a recovery operation.

6366
Paula

Verifying Archive Results

During a system recovery, Ignite-UX strives to restore the system back to the way it was. However, Ignite-UX is a general-purpose installation tool, and can modify many system configuration files.

When you run `make_net_recovery`, a lot of system configuration information is gathered and saved in config files that are used later when the system is recovered. During the system recovery the user is allowed to make changes to this information, in which case Ignite-UX will make the appropriate changes to the system configuration. If a user does not make any changes, then it simply re-applies the same information and you should see no change to the system in the end.

Most of the system configuration files that Ignite-UX will modify are listed in the script: `/opt/ignite/data/scripts/os_arch_post_l`. The `os_arch_post_l` script checks for the system recovery case by checking the `$RECOVERY_MODE` variable. When this variable is TRUE, the os_arch_post_l script causes some configuration files to be protected from modification by using the "save_file" function. os_arch_post_l uses the "merge_file" function on files that Ignite-UX knows how to intelligently merge information into.

The files operated on by "merge_file", as well as those that have a commented out "save_file" line are those that are likely to be modified by Ignite-UX. Comments in the file explain any exceptions.

Because the list of files modified by Ignite-UX may change from release-to-release, it is best to look at the os_arch_post_l file on your system to see which files are saved as-is and which are merged with information from the Ignite-UX config files.

Retaining "Known-good" Archives

You may want to prevent known-good archives from being deleted from your system. `make_net_recovery` provides the -n option to specify the number of archives to save. To preserve disk space, the oldest archive(s) are removed as new archives are created. The number of archives that get removed is based on the number of archives specified to be saved.

One way to ensure that known-good archives are saved would be to specify the number of archives to save to be greater then the maximum number of archives you plan to store on the system at any given time. This would cost disk space.

An alternative and better approach to saving known-good archives is to rename the archive and edit the configuration file to include the new archive name. Follow these steps:

Step 1. Login to the system where the archive is to be stored (this could be different than the Ignite-UX server).

Step 2. Rename the archive. (The path to the archive may be different than the example below). The name of the archive to save can be anything unique, but it should be outside the naming convention: *yyyy-mm-dd,hr:min*

```
cd /var/opt/ignite/recovery/archives/system_name
mv old_archive_name saved_archive_name
```

For example:

```
mv 2001-05-11,15:14 Recovery_Archive.0511.save
```

Step 3. If the archive server is different from the Ignite-UX server, login to the Ignite-UX server system.

6364 Paula

Step 4. Edit this file to reference new archive name:

```
/var/opt/ignite/clients/client/recovery/  \
old_archive_name/archive_cfg
```

Change the `archive_path` variable inside the `(source_type == "NET")` conditional to the name of the saved archive. For example:

```
(source_type == "NET") {
  archive_path = "Recovery_Archive.0511.save"
}else {
  archive_path = "1"
}
```

Step 5. Optionally, edit the `cfg` tag entry in the file:

/var/opt/ignite/clients/`client`*/CINDEX*

so that configuration will be unique and descriptive when it is viewed via the Ignite-UX screen. For example:

Change from:

```
cfg "2001-05-13,06:51 Recovery Archive" {
description "Weekly System Recovery Archive"
...

}
```

To:

```
cfg "Saved Recovery Archive" {
description "Weekly System Recovery Archive"
...

}
```

Making config File Additions

To make configuration file additions to all recovery configurations for a given client, create a new Ignite-UX configuration file called:

```
/var/opt/ignite/clients/0x{LLA}/recovery/config.local
```

For local tapes the file is located in:

```
/var/opt/ignite/recovery/config.local
```

This `config.local` file will automatically be included into your recovery configuration for this client each time you run `make_net_recovery`. (`make_net_recovery` is run for you when you use Ignite-UX for network recovery).

If you already have recovery configurations for this client and would like them to include the `config.local` file, edit the `/var/opt/ignite/clients/0xLLA/CINDEX` file to include a reference to "recovery/config.local" in all of the configuration clauses.

E 6362 Paula

Selecting File Systems During Recovery

It is possible to change the way your disks are configured when you recover from an image saved by `make_net_recovery`.If you want to use a standard HP filesystem layout, you can specify the disk configuration using Ignite-UX:

Install Client –> New Install –> File System

If you do not want to use a standard HP filesystem layout, you can modify the `/var/opt/ignite/clients/0x`*`LLA`*`/CINDEX` file for the client you are recovering. The `CINDEX` file contains one or more configuration clauses that refer to the recovery images you have previously created with `make_net_recovery`. Add a new configuration file entry to the clause that you intend to recover from. If you want to add HP's standard file system choices, add the file:

`/opt/ignite/data/Rel_`*`release`*`/config`

Where: *release* is the operating system release on the client you intend to recover. For example:

`/opt/ignite/data/Rel_B.10.20/config`

would be added for a client with the HP-UX 10.20 operating system. This new configuration file entry should be the first entry in the clause you are modifying.

When you bring up the user interface during recovery, select the File System type you wish to use on the **Basic** tab.

Tape Recovery with make_net_recovery

There are two ways you can recover from a tape with `make_net_recovery`. The method you choose depends on your needs.

Use make_medialif This method is useful when you want to create a totally self-contained recovery tape. The tape will be bootable and will contain everything needed to recover your system, including the archive of your system. During recovery, no access to an Ignite-UX server is needed. Using `make_medialif` is described beginning on page 180 and also on the Ignite-UX server in the file: `/opt/ignite/share/doc/makenetrec.txt`

Use make_boot_tape This method is useful when you do not have the ability to boot the target machine via the network, but are still able to access the Ignite-UX server via the network for your archive and configuration data. This could happen if your machine does not support network boot or if the target machine is not on the same subnet as the Ignite-UX server. In these cases, use `make_boot_tape` to create a bootable tape with just enough information to boot and connect with the Ignite-UX server. The configuration files and archive are then retrieved from the Ignite-UX server. See the *make_boot_tape* (1M) manpage for details.

6360 Paula

Tape Recovery with No Tape Boot Support

You can use the Ignite-UX tape recovery tool to archive your system even if there is no tape boot support on the system. This support is provided in the Ignite-UX B.4.1 release and later only.

IMPORTANT Be sure to locate the December 2002 version or later of Ignite-UX (B.4.1 or later) media (CD or DVD) that can be used to boot your system to the interface screens to guide you through tape recovery using a tape drive.

Step 1. Insert the December 2002 version or later of Ignite-UX (B.4.1 or later) media into the appropriate drive, then boot from it.

The following interface screen appears:

```
                User Interface and Media Options

   This screen lets you pick from options that will determine if an
   Ignite-UX server is used, and your user interface preference.

Source Location Options:
   [ * ]  Media only installation
   [   ]  Media with Network enabled (allows use of SD depots)
   [   ]  Ignite-UX server based installation

 User Interface Options:
   [ * ]  Guided Installation   (recommended for basic installs)
   [   ]  Advanced Installation (recommended for disk and file
system management)
   [   ]  No user interface - setup basic networking, use defaults
and go
   [   ]  Remote graphical interface running on the Ignite-UX server

   Hint: If you need to make LVM size changes, or want to set the
         final networking parameters during the install, you will
         need to use the Advanced mode (or remote graphical
interface).


   [   OK   ]            [ Cancel ]              [  Help  ]
```

Step 2. Click the **OK** button to continue and you are advanced to the next screen:

```
                    Media Installation

  This screen provides an option to switch the install source
from the default CD/DVD to a recovery tape.  This is helpful
for those systems and for tape devices which do not support
booting from a tape.

   [   ] CD/DVD Installation
   [ * ] Boot from CD/DVD, Recover from Tape


   [ OK ]      [ cancel ]    [ Help ]
```

Step 3. Select the **Boot from CD/DVD, Recover from Tape** and click **OK** to advance to the Tape Drive Selection screen:

```
                      Tape Drive Selection

  There are one or more tape drives detected on the system.
Insert your recovery tape into one of the drives and then
select that drive from the list below.

    Use the <tab> and/or arrow keys to move to the desired
TAPE device
    to enable, then press <Return/Enter>.

        HW Path              Device File
Description

-------------------------------------------------------------

      [ 0/18/1/0/0.0.3.0    /dev/rmt/c0t0d0          HP C5683A ]
      [ 0/18/1/0/0.1.0.0    /dev/rmt/c1t1d1          HP A5580A ]
```

Step 4. Select the tape drive that contains the archive tape then press **Enter** to start the installation of the recovery tape archive from the chosen tape drive.

Notes on Cloning Systems

Ignite-UX offers two main options for replicating (cloning) systems. The traditional Ignite-UX method makes use of make_sys_image to create an archive of the source system, followed by manually modifying config files to meet your needs. A much simpler (but less flexible approach) uses make_net_recovery or make_tape_recovery. The pros and cons of each are described here.

In each case, the source system that is used must contain software that is compatible with all target systems. This means that the version of HP-UX, patches, drivers, etc., must be sufficient for all systems involved. This often requires loading a superset of software and drivers onto the source system that will be used on all potential targets.

Using make_sys_image

Using the traditional method of creating an archive with make_sys_image and then modifying Ignite-UX configuration files to reference the archive is very flexible, but somewhat time consuming. The end result gives you:

- Ability to install systems from network, tape, or CD-ROM from either an Ignite-UX server, or local clients.
- Ability to customize the process and tune it to accommodate many different situations.
- A "clean" system — log files and most remnants specific to the source system are removed.
- A rebuilt kernel containing just the drivers needed by the target system's hardware.
- Ability to load additional software or patches on top of the system archive from an SD depot. This reduces the need to recreate the archive, and allows you to add support for new hardware that requires new patches, or drivers without making a new archive.

Using make_net_recovery and make_tape_recovery

The make_tape_recovery and make_net_recovery tools are designed to reproduce a system exactly the way it was at the time the snapshot was taken. These tools try to accommodate for cloning in various ways:

- You can change hostname/networking information.
- You can make changes to disks and file systems during the recovery.

- Detect hardware model changes and rebuild the kernel.

However, their attempt to reproduce a system exactly may be undesirable:

- The disk layout is saved "as-is" from the original system and does not have flexible logic to accommodate disks of varying sizes or locations.
- Hardware instance numbers for devices that exist at the same paths between systems have the instance numbers preserved from the original system. This can cause non-contiguous assignments in instance numbers. Which is usually only a cosmetic problem.
- Many files that are specific to the system the recovery image was taken from, are preserved. This includes many log files, etc.
- When the kernel is rebuilt (in the "cloning" situation), drivers may be added as needed by the hardware, but unused drivers will not be removed.

The next section shows how to clone a system using make_net_recovery. System cloning using make_tape_recovery begins on page 169.

Cloning a System Using make_net_recovery

The recovery configurations and archives created by make_net_recovery are stored in a separate directory on the Ignite-UX server for each client. Using the configuration and archive created by make_net_recovery on one system to install a different system involves manually copying some configuration files, and allowing NFS access to the source system's archive. Follow these steps:

Step 1. Use make_net_recovery or Ignite-UX to create a system recovery archive of the source system.

Step 2. Login to the Ignite-UX server.

Step 3. If the target system to be installed does not currently have a directory in /var/opt/ignite/clients but is up and running, then use Ignite-UX to create that directory using **Actions –> Add New Client for Recovery**. If the system is not running, you will either need to boot the client from the Ignite-UX server (or from a tape made with make_boot_tape in order for this directory to be created.

Step 4. Copy the `CINDEX` and recovery directory from the source client to the target client directory. If the target client has previously used `make_net_recovery` then it will already have a `CINDEX` file. If the `CINDEX` file for the target system exists already, you may want to save a copy, and/or hand edit the file to add the desired entries from the source client. The commands below copy the required files. You may specify `src_client` and `target_client` using either the LAN addresses (such as 0x0060B04AAB30), or by using the client's hostname (which is a symlink to the LAN address):

```
cd /var/opt/ignite/clients/src_client
find CINDEX recovery | cpio -pdvma ../target_client
```

Step 5. Give the *target_client* NFS access to the archive of the source system. To do this, login to the server that holds the archive (normally the Ignite-UX server).

Typically each client has its own directory for storing the archives, and the directory is exported only to the individual client. In this case, you will need to edit the `/etc/exports` file to allow access to both the source and target clients:

1. Enter: **`vi /etc/exports`**

2. Append **`:target-client`** to the end of the source-client's line.

3. Enter: **`exportfs -av`**

Step 6. Boot the target-client from the Ignite-UX server (using any method you wish). Then when you install the system, you can select from the recovery configurations of the source system.

Step 7. Change the system networking parameters for the target system during the installation.

Expert Recovery Using the Core Media

If your system should become so compromised or corrupt that it will not boot at the login prompt, or the system boots, but critical files are corrupted, adversely affecting overall system performance, it may be useful to restore system elements with core recovery media.

Before you attempt to recover an HP-UX system, you should have the following information about your system disk available.

Much of this information, including file system types, can be obtained by accessing your on-line system manifest, either via Ignite-UX, or by reading the hardcopy that came with your system

- Revision of the HP-UX system which you are attempting to recover.

CAUTION Only attempt to recover HP-UX systems that match the version number of the recovery tools you are using, currently HP-UX 11.0. For example, you can use HP-UX 10.20 Core media to attempt to recover an HP-UX 10.20 file system.

- The hardware path of the root filesystem on the disk (that is, what file system you will be checking/repairing using `fsck`).
- The address of the bootlif path of that disk.
- What the autofile in the bootlif should contain.
- Whether you have an LVM, VXVM, or whole-disk system.

The more you know about the system disk and its partitioning scheme, *before you encounter major damage or corruption*, the easier it will be for you to recover.

The procedures which follow assume that both `fsck` and `mount` can be run successfully on the system disk; otherwise, the following procedures are not applicable.

6334 folha

Automated Recovery Procedures

There are four possible expert recovery situations, each of which has its associated recovery procedure:

- If, after a system problem, you can't get the system to the `ISL>` prompt from the system disk, you will want to rebuild the bootlif on the system disk, and install all critical files required to boot on the root filesystem.
- If you can get the system to the `ISL>` prompt, but cannot boot `vmunix`, the system disk is corrupted; you will want to install *only* the critical files required to boot on the root filesystem.
- If you can't get to the `ISL>` prompt, but you know that the root file system is good, you will want to rebuild the bootlif on the system disk.
- If you believe your kernel is corrupted, you will want to replace only the kernel on the root filesystem.

The following subsections describe these procedures in detail.

Rebuilding the bootlif and Installing Critical Files

Following is an example of the detailed procedure for rebuilding the bootlif of the system disk, and for installing all the critical files necessary to boot from the root filesystem:

Step 1. Have the Core OS CD for the appropriate HP-UX ready.

Step 2. Reset the System Processor Unit (SPU) using the reset button, or keyswitch, as appropriate.

The console displays boot path information. If Autoboot is enabled, the system console eventually displays messages similar to this:

```
Autoboot from primary path enabled
To override, press any key within 10 seconds.
```

Step 3. With older systems, press any key within 10 seconds. The system console displays:

```
Boot from primary boot path (Y or N)?>
```

Enter **n** at the prompt. The next prompt is:

```
Boot from alternate boot path (Y or N)?>
```

Step 4. If the alternate boot path specifies the address of the CD device where the Core CD is mounted, enter: **y**

If the alternate boot path does not specify the address of the CD device where the HP-UX Core media is mounted, enter **n** at the prompt. The next prompt is:

```
Enter boot Path or ?>
```

Step 5. Enter the address of the CD device where the HP-UX Core media is mounted. The next prompt is:

```
Interact with IPL (Y or N)>
```

Step 6. Enter **n** at the prompt.

After several minutes and several screens of status information, the this is displayed:

```
Welcome to the HP-UX installation/recovery process!
Use the <tab> and/or arrow keys to navigate through the
following menus,and use the <return> key to select an item. If
the menu items are not clear, select the "Help" item for more
information.

                    [    Install HP-UX        ]
                    [  Run a Recovery Shell   ]
                    [   Advanced Options      ]
                                 [ Help ]
```

Step 7. Select: **Run a Recovery Shell**. The next prompt is:

```
Would you like to start up networking at this time? [n]
```

Step 8. Unless you need networking to ftp to other systems, enter: **n**

```
* Loading in a shell...
* Loading in the recovery system commands...
             HP-UX SYSTEM RECOVERY CORE MEDIA
             WARNING:  YOU ARE SUPERUSER !!
NOTE: Commands residing in the RAM-based file system are unsupport
ed 'mini'commands. These commands are only intended for recovery p
urposes.

Loading commands needed for recovery!

Press <return> to continue.
```

Step 9. Press **Return** or **Enter**. The next prompt is:

```
Loading commands needed for recovery!
```

This menu is displayed:

```
HP-UX CORE MEDIA RECOVERY
   MAIN MENU
 s.  Search for a file
 b.  Reboot
 l.  Load a file
 r.  Recover an unbootable HP-UX system
 x.  Exit to shell

This menu is for listing and loading the tools contained
on the core media.  Once a tool is loaded, it may be run
from the shell. Some tools require other files
to be present in order to successfully execute.
Select one of the above:
```

Step 10. To load a file or files, enter `l` at the prompt.

```
Filesystem kbytes used avail %cap iused ifree iused Mounted on
/                 2011    1459 552  73%   137    343 29%   ?
/duped_root       2011    1418 593  71%    49    431 10%   ?
Enter the filename(s) to load:
```

Step 11. Enter the name(s) of the damaged/corrupted file(s) you wish to load. For example:

`sh vi date grep`

The following example lists two files (ex and egrep) which must be loaded before the files `vi` and `grep` can be loaded. It also lists a file (`date`) which is not in the load list.

```
NOTE :
  Since ./usr/bin/vi is linked to ./usr/bin/ex
  './usr/bin/ex' must precede './usr/bin/vi' in the load list.
The file 'date' is NOT in the LOADCMS archive.
<Press return to continue>
NOTE :
Since ./usr/bin/grep is linked to ./usr/bin/egrep
'./usr/bin/egrep' must precede './usr/bin/grep' in the loadlist.
********  THE REQUESTED FILE(S): ***********
./sbin/sh ./usr/bin/vi ./usr/bin/grep
Is the above load list correct? [n]
```

Step 12. This load list is incorrect, because `./usr/bin/ex` does not precede `./usr/bin/vi` in the list of requested files. So you would enter: **n**

```
Nothing will be loaded!
<Press return to return to Main Menu>
```

Step 13. Press **Enter** and the Main Menu appears. To search for a file you wish to load, select: **s**

```
Either enter the filename(s) to be searched for,
or 'all' for a total listing.
```

Step 14. Enter:

```
vi awk /sbin/sh date
```

You will receive this response:

```
./usr/bin/vi linked to ./usr/bin/ex
./sbin/awk
./usr/bin/awk
./sbin/sh
**** The file  'date' was not found in the LOADCMDS archive. ****
<Press return to continue>
```

Step 15. Press **Enter** to return to the Main Menu.

Step 16. To begin the actual system recovery and invoke the Recovery Menu, select: **r**

```
 HP-UX Recovery MENU
 Select one of the following:
a. Mount the root disk and exit to shell only.
b. Recover the bootlif/os partitions.
c. Replace the kernel on the root file system.
d. Both options b and c

v. Read information about VxVM/LVM recovery

m. Return to 'HP-UX Recovery Media Main Menu'.
x. Exit to the shell.
```

Step 17. To install both the bootlif and critical files, select: **a**

```
DEVICE FILE VERIFICATION MENU
This menu is used to specify the path of the root file sysem.
When the information is correct, select 'a'.

INFORMATION to verify:
       Device file used for '/'(ROOT) is c1t6d0
       The path to disk is 56/52.6.0
 Select one of the following:
  a.  The above information is correct.
  b.  WRONG!! The device file used for '/'(ROOT) is incorrect.
  m.  Return to the 'HP-UX Recovery MENU.'
  x.  Exit to the shell.
```

Step 18. Assuming the root device file is incorrect, select: **b**

```
Enter the device file associated with the '/'(ROOT)

file system. (example: c1t6d0):
```

On a system with hard-sectored disks, the prompt and response might look like this:

```
Enter the device file associated with the '/'(ROOT) file system
(example: c0t1d0s1lvm ) :  c0t0d0s13
/dev/rdsk/c0t0d0s13 not a special file
<Press return to continue>
Enter the address associated with the '/'(ROOT) file system
(example: 4.0.1) :  4.0.0
NOTE: if your '/'(ROOT) is not part of a sectioned disk layout
    enter a 'W' for whole disk layout
       or
    enter a 'l' for an LVM disk layout
  instead of a section number.
Enter the section associated with the '/'(ROOT) file system
(example: 13 ):  13
 making rdsk/c0t0d0s13 c 214 0x00000d
 making dsk/c0t0d0s13 b 26 0x00000d
```

Step 19. If you entered **c1t1d0** as the root device filename, you would see:

```
DEVICE FILE VERIFICATION MENU
This menu is used to specify the path of the root file
system When the information is correct, select 'a'.
INFORMATION to verify:
       Device file used for '/'(ROOT) is c1t1d0
       The path to disk is 56/52.1.0
 Select one of the following:
    a.  The above information is correct.
    b.  WRONG!! The device file used for '/'(ROOT) is incorrect.
    m.  Return to the 'HP-UX Recovery MENU.'
    x.  Exit to the shell.
```

Step 20. Since c1t1d0 is the correct root device filename, select: **a**

```
BOOTLIF PATH VERIFICATION MENU
This menu must be used to determine the path to the bootlif(ISL, H
PUX and the AUTO file).
When the information is correct, select 'a'.
INFORMATION to verify:
      Path to the bootlif is 56/52.1.0
Select one of the following:
      a.  The above information is correct.
      b.  WRONG!! The path to bootlif is incorrect.
      m.  Return to the 'HP-UX Recovery MENU.'
      x.  Exit to the shell.
     Selection:
```

Step 21. Assuming that the bootlif path is correct, enter: **a**

```
FILE SYSTEM CHECK MENU

The file system check'/sbin/fs/hfs/fsck -y /dev/rdsk/c1t10'
will now be run.
Select one of the following:
      a.  Run fsck -y .
      b.  Prompt for the fsck run string on c1t1d0.
      m.  Return to the 'HP-UX Recovery MENU.'
     Selection:
```

Step 22. Select **a** to run **`fsck -y`** to check your file system for corruption.

```
** /dev/rdsk/c1t1d0
** Last Mounted on /ROOT
** Phase 1 - Check Blocks and Sizes
** Phase 2 - Check Pathnames
** Phase 3 - Check Connectivity
** Phase 4 - Check Reference Counts
** Phase 5 - Check Cyl groups
6256 files, 0 icont, 149423 used,1563824 free(928 frags,195362 blo
cks)
Mounting c1t1d0 to the HP-UX Recovery Media /ROOT directory...
<Press return to continue>
```

Step 23. Assuming your file system is not corrupted, and you wish to continue with the system recovery, press **Return** to mount your root file system under the / directory. You'll see messages like this:

```
   ***** Downloading files to the target disk *****
x ./sbin/lvchange, 528384 bytes, 1032 tape blocks
./sbin/lvcreate linked to ./sbin/lvchange
./sbin/lvdisplay linked to ./sbin/lvchange


Filesystem kbytes used avail %cap iused ifree iused Mounted on
/ROOT    1713247  149426 1392496  10%  6261 275339  2%   ?

Should the existing kernel be
'left', 'overwritten', or 'moved'?[overwritten]
```

Step 24. To overwrite the existing kernel with your new file system, enter **`overwritten`** or **over** at the prompt.

```
 downloading INSTALL to /stand/vmunix
    **** Creating device files on the target disk ****
    ******* Renaming the following files: *******
     '/.profile' has been renamed '/.profileBK'
      *********** Installing bootlif  ***********
mkboot -b /dev/rmt/1m  -i ISL -i HPUX /dev/rdsk/c1t1d0
mkboot -a  hpux (56/52.1.0;0)/stand/vmunix /dev/rdsk/c1t1d0
```

Step 25. Complete the recovery process by selecting: **a**

```
NOTE:    System rebooting ...
-
PDC - Processor Dependent Code - Version   1.3
(c) Copyright 1990-1993, Hewlett-Packard Company, All rights
reserved.
-
   16 MB of memory configured and tested.
   Primary boot path:     56/52.5     (dec)
   Alternate boot path:  56/52.3     (dec)
Manufacturing permissions ON
-    Main Menu
Command                           Description
        -                             -
BOot [PRI|ALT| &<path>]          Boot from specified path
PAth [PRI|ALT|] [ &<path>]       Display or modify a path
SEArch [DIsplay|IPL] [&<path>] Search for boot devices
COnfiguration menu      Displays or sets boot values
INformation menu        Displays hardware information
SErvice menu            Displays service commands
MFG menu                Displays manufacturing commands

DIsplay                 Redisplay the current menu
HElp [&<menu>|&<command>] Display help for menu or command
RESET                   Restart the system
-
Main Menu: Enter command or menu item.
```

Step 26. Enter **bo pri** at the prompt to boot from the primary boot path. The next prompt is:

```
Interact with IPL (Y or N)?>
```

Step 27. Enter **n** for unattended boot. Several screens of status information are displayed, followed by this warning:

```
THIS SYSTEM HAS BEEN BOOTED USING A TEMPORARY KERNEL!
DO NOT ATTEMPT TO INVOKE MULTI-USER RUN-LEVEL USING THIS KERNEL!
Type the following command from the shell prompt for more
information about completing the recovery process:

cat /RECOVERY.DOC
```

Step 28. To obtain more information on the recovery process, enter:

```
cat /RECOVERY.DOC
```

```
1) Restore valid copies of the following files (either from backup
 or
   from the filename.BK files created during the recovery process)
.
   /etc/fstab,        /etc/inittab,  /stand/ioconfig,
   /etc/ioconfig,      /etc/passwd,  /sbin/pre_init_rc,
   /.profile,   and /etc/profile
  NOTE:  The backup archive may be extracted using '/sbin/frecover
' or'/sbin/pax' (for backups made with 'tar' or 'cpio').
If using '/sbin/pax', linking it to 'tar' or 'cpio' will
force'pax' to emulate the respective command line interface.
2) Replace /stand/vmunix from backup, since the present kernelis p
robably missing desired drivers.
3) If you have an lvm root, refer to the /LVM.RECOVER text file.
```

Step 29. If you have an LVM system, and want more information on recovery procedures, enter:

```
cat /LVM.RECOVER
```

Follow the displayed instructions shown below.

NOTE If a card has been added to, or removed from, your system since the original installation was completed, there is a chance that the device file for the root disk has changed. Consequently, before you run the LVM script *./lvmrec.scrpt* (Step 2 in the displayed instructions below), you should first recover */stand/ioconfig* from backup, and reboot.

```
INSTRUCTIONS to complete your LVM recovery:
The system must now be up now in "maintenance mode".
NOTE: In order for the following steps to lead to a successful
      lvm recovery the LVM label information must be valid.
      If the bootlif was updated from the RAM-based recovery syste
m,
      then "mkboot -l" has already been run to repair this label.
step 1. If the autofile was altered to force the system to boot in
 maintenance mode, use "mkboot -a" to remove the "-lm" option.
 Example:
    to change  "hpux -lm (52.6.0;0)/stand/vmunix"
    to   "hpux   (52.6.0;0)/stand/vmunix"
    use
   mkboot -a  "hpux (52.6.0;0)/stand/vmunix"  /dev/rdsk/<device fi
le>
```

(Use `lssf /dev/rdsk/*` to match the device file with the boot address.)

```
step 2. Run '/lvmrec.scrpt' to repair the following LVM
 configuration information:
        a. LVM records (lvmrec)
        b. BDRA (Boot Data Reserve Area)
        c. LABEL information
 Requirement:  The following files must reside on disk before
        the script can complete:
        a. /etc/lvmtab
        b. /etc/fstab
        c. /etc/lvmconf/<rootvg>.conf
        d. all device files specified in /etc/fstab
 To run '/lvmrec.scrpt' provide the device filename used to
 access the bootlif as an argument to the script.
 Example:
  /lvmrec.scrpt c0t6d0
  In this example 'c0t6d0' is the device file used to
  access the bootlif.
step 3. Once '/lvmrec.scrpt' completes, issue the command "reboot"
 and bringthe system fully up.
 The recovery of the root LVM is complete.  If the'/lvmrec.scrpt'
issued the following warning:
  "************* I M P O R T A N T *****************          "Root
 logical volume has been repaired, but......."
  "you need to reboot the system and repair the Swap"
  "logical volume using the following LVM command:  "
  "   lvlnboot -A n -s /dev/<root lv>/<swap lvol>   "
  "because Recovery has no way to find out what is  "
  "the Swap logical volume information at this point"
  "*************************************************"

The Swap and Dump logical volumes will need to be re-configured
The BDRA contains the "root", "swap" and "dump" logical volumeinfo
rmation. '/lvmrec.scrpt' only fixes the root logical volume
information in the BDRA.The "swap" and "dump" areas can be updated
via the "lvlnboot" command.

 Example:
    lvlnboot -s /dev/<vg00>/lvol2
    lvlnboot -d /dev/<vg00>/lvol3
 In this example 'lvol2' and 'lvol3' are the "swap" and "dump"
  logical volumes respectively.

step 4. Perform any further data recovery deemed necessary.
```

```
*** NOTE ***
If the same volume group contains more than one corrupted bootdisk
, Repeat the above steps for each disk that needs to be repaired.
```

This completes the process for rebuilding the bootlif and installing critical files.

Installing Critical Root Files Only

Following is an example of the detailed procedure for installing all the critical files necessary to boot on the target root file system:

Boot the Core media, following the steps in Chapter 2. You will see some status messages, and then a menu:

```
Welcome to the HP-UX installation process!
Use the <tab> and/or arrow keys to navigate through the following
menus,and use the <return> key to select an item.  If the menu ite
ms are not clear, select the "Help" item for more information.

                     [    Install HP-UX       ]
                     [  Run a Recovery Shell  ]
                     [   Advanced Options     ]
                                   [ Help ]
```

Step 1. Select **Run a Recovery Shell**, the screen clears, and the following question appears:

```
Would you like to start up networking at this time? [n]
```

Step 2. If you have no need to access the net, enter: **n**

```
* Loading in a shell...
* Loading in the recovery system commands...
(c) Copyright 1983, 1984, 1985, 1986 Hewlett-Packard Co.
(c) Copyright 1979 The Regents of the University of Colorado,
a body corporate
(c) Copyright 1979, 1980, 1983 The Regents of the
      University of California
(c) Copyright 1980, 1984 AT&T Technologies.  All Rights Reserved.
                         HP-UX SYSTEM RECOVERY CORE MEDIA
                         WARNING:  YOU ARE SUPERUSER !!
NOTE: Commands residing in the RAM-based file system are unsupport
ed 'mini' commands. These commands are only intended for
recovery purposes.
Loading commands needed for recovery!
WARNING: If ANYTHING is changed on a root (/) that is mirrored,
'maintenance mode' (HPUX -1m) boot MUST be done in order to force
the mirrored disk to be updated!

Press <return> to continue.
```

Step 3. Press: **Return**

```
Loading commands needed for recovery!

Then the following menu will be displayed:
```

6342 Paula

```
HP-UX CORE MEDIA RECOVERY
   MAIN MENU
 s.  Search for a file
 b.  Reboot
 l.  Load a file
 r.  Recover an unbootable HP-UX system
 x.  Exit to shell
 c.  Instructions on chrooting to a lvm /(root).
This menu is for listing and loading the tools contained
on the core media.  Once a tool is loaded, it may be run
from the shell. Some tools require other files to be preset
in order to successfully execute.
Select one of the above:
```

Step 4. To begin the actual system recovery, select **r** to see the HP-UX Recovery Menu:

```
 HP-UX Recovery MENU
 Select one of the following:
a. Mount the root disk and exit to shell only.
b. Recover the bootlif/os partitions.
c. Replace the kernel on the root file system.
d. Both options b and c

v. Read information about VxVM/LVM recovery

m. Return to 'HP-UX Recovery Media Main Menu'.
x. Exit to the shell.
```

Step 5. To install critical files only, select: **b**

```
DEVICE FILE VERIFICATION MENU
   This menu is used to specify the path of the root file system.
   When the information is correct, select 'a'.
 INFORMATION to verify:
       Device file used for '/'(ROOT) is c1t6d0
       The path to disk is 56/52.6.0
 Select one of the following:
       a.  The above information is correct.
       b.  WRONG!! The device file used for '/'(ROOT) is incorrect
       m.  Return to the 'HP-UX Recovery MENU.'
       x.  Exit to the shell.
```

Step 6. Assuming the root device file is incorrect, select **b**; you will be prompted to enter the correct device filename:

```
 Enter the device file associated with the '/'(ROOT) file system
 (example: c1t6d0):
```

On a system with hard-sectored disks, the prompt and response might look like this:

```
Enter the device file associated with the '/'(ROOT) file system
(example: c0t1d0s1lvm ) :  c0t0d0s13
/dev/rdsk/c0t0d0s13 not a special file
<Press return to continue>
Enter the address associated with the '/'(ROOT) file system
(example: 4.0.1) :  4.0.0
   NOTE: if your '/'(ROOT) is not part of a sectioned disk layout
    enter a 'W' for whole disk layout
       or
    enter a 'l' for an LVM disk layout
  instead of a section number.
 Enter the section associated with the '/'(ROOT) file system
 (example: 13 ):  13
 making rdsk/c0t0d0s13 c 214 0x00000d
 making dsk/c0t0d0s13 b 26 0x00000d
```

Step 7. If you were to enter, for example, **c1t1d0** as the root device filename, you would see this:

```
DEVICE FILE VERIFICATION MENU
   This menu is used to specify the path of the root file system.
   When the information is correct, select 'a'.
 INFORMATION to verify:
       Device file used for '/'(ROOT) is c1t1d0
       The path to disk is 56/52.1.0
 Select one of the following:
       a.  The above information is correct.
       b.  WRONG!! The device file used for '/'(ROOT) is incorrect
       m.  Return to the 'HP-UX Recovery MENU.'
       x.  Exit to the shell.
```

Step 8. Since c1t1d0 is the correct root device filename, select: **a**

```
FILE SYSTEM CHECK MENU
   The file system check '/sbin/fs/hfs/fsck -y /dev/rdsk/c1t1d0'
   will now be run.
 Select one of the following:
      a.  Run fsck -y .
      b.  Prompt for the fsck run string on c1t1d0.
       m.  Return to the 'HP-UX Recovery MENU.'
```

6340
Paula

Step 9. Select **a** to run **`fsck -y`** to check your file system for corruption.

```
** /dev/rdsk/c1t1d0
** Last Mounted on /ROOT
** Phase 1 - Check Blocks and Sizes
** Phase 2 - Check Pathnames
** Phase 3 - Check Connectivity
** Phase 4 - Check Reference Counts
** Phase 5 - Check Cyl groups
6256 files, 0 icont, 149423 used, 1563824 free (928 frags, 195362
blocks)
Mounting c1t1d0 to the CORE media /ROOT directory...
<Press return to continue>
```

Step 10. Assuming your file system is not corrupted, and you wish to continue with the system recovery, press **Return** to mount your root file system under the Core media / directory.

```
   ***** Downloading files to the target disk *****
x ./sbin/lvchange, 528384 bytes, 1032 tape blocks
./sbin/lvcreate linked to ./sbin/lvchange
./sbin/lvdisplay linked to ./sbin/lvchange
./sbin/lvextend linked to ./sbin/lvchange
                ...
Filesystem      kbytes    used   avail %cap iused  ifree iused Mou
nted on
/ROOT       1713247  149426 1392496  10%  6261 275339  2%   ?
Should the existing kernel be
'left', 'overwritten', or 'moved'?[overwritten]
```

Step 11. To overwrite the existing kernel with your new file system, enter **`overwritten`** or **`over`** at the prompt.

```
 downloading INSTALL to /stand/vmunix
    **** Creating device files on the target disk ****
    ******* Renaming the following files: *******
     '/.profile' has been renamed '/.profileBK'
    RECOVERY COMPLETION
    MENU
     Use this menu after the recovery process has installed all re
quested
     files on your system.
 Select one of the following:
      a.  REBOOT the target system and continue with recovery.
       b.  Return to the CORE Media Main Menu.
```

Step 12. Complete the recovery process by selecting: **a**

```
NOTE:    System rebooting...
   PDC - Processor Dependent Code - Version   1.3
   (c) Copyright 1990-1993, Hewlett-Packard Company,
        All rights reserved
    16 MB of memory configured and tested.
    Primary boot path:      56/52.5    (dec)
    Alternate boot path:    56/52.3    (dec)
Manufacturing permissions ON
- Main Menu -
        Command                        Description
        -                      -
        BOot  [PRI|ALT|<path>]       Boot from specified path
        PAth  [PRI|ALT]  [<path>]      Display or modify a path
        SEArch [DIsplay|IPL]  [<path>] Search for boot devices

        COnfiguration menu          Displays or sets boot values
        INformation menu            Displays hardware information
        SERvice menu                Displays service commands
        MFG menu                    Displays manufacturing commands
        DIsplay                     Redisplay the current menu
        HElp [<menu>|<command>]     Display help for menu or command
        RESET                           Restart the system
- Main Menu: Enter command or menu >
```

Step 13. Enter **bo pri** at the prompt to boot from the primary boot path.

```
Interact with IPL (Y or N)?>
```

Step 14. Enter **n** for unattended boot; several screens of status information will be displayed, followed by this warning:

```
THIS SYSTEM HAS BEEN BOOTED USING A TEMPORARY KERNEL!
DO NOT ATTEMPT TO INVOKE MULTI-USER RUN-LEVEL USING THIS KERNEL!
Type the following command from the shell prompt for more informat
ion
about completing the recovery process:
cat /RECOVERY.DOC
```

Step 15. To obtain more information on the recovery process, enter:

cat /RECOVERY.DOC

```
1) Restore valid copies of the following files (either from backup
 or
   from the <filename>BK files created during the recovery process
).
   /etc/fstab,       /etc/inittab,  /stand/ioconfig,
   /etc/ioconfig,     /etc/passwd,  /sbin/pre_init_rc,
   /.profile,    and /etc/profile
  NOTE:  The backup archive may be extracted using '/sbin/frecover
' or
   '/sbin/pax' (for backups made with 'tar' or 'cpio').
 If using '/sbin/pax', linking it to 'tar' or 'cpio' will force 'p
ax'
```

6338 Paula

```
    to emulate the respective command line interface.
2) Replace /stand/vmunix from backup, since the present kernel is
probably missing desired drivers.
3) If you have an lvm root, refer to /LVM.RECOVER .
```

Step 16. If you have an LVM system, and want more information on recovery procedures, enter:

`cat /LVM.RECOVER`

The file contains the following information:

```
If a card has been added to, or removed from, your system
since the original installation was completed,
there is a chance that the device file for the root disk has chang
ed.
Consequently, before you run the LVM script ./lvmrec.scrpt
(Step 2, below), you should first recover /stand/ioconfig
from backup and reboot.
INSTRUCTIONS to complete your LVM recovery:
The system must now be up now in "maintenance mode".
NOTE: In order for the following steps to lead to a
successful lvm recovery the LVM label information must be valid.
If the bootlif was updated from the RAM-based recovery system,
then "mkboot -l" has already been run to repair this label.

step 1. If the autofile was altered to force the system to boot in
 maintenance mode, use "mkboot -a" to remove the "-lm" option.
 Example:
    to change  "hpux -lm (52.6.0;0)/stand/vmunix"
    to   "hpux   (52.6.0;0)/stand/vmunix"
    use
   mkboot -a "hpux (52.6.0;0)/stand/vmunix"/dev/rdsk/<device file>
```

NOTE To match device file with boot address, use: **`lssf /dev/rdsk/*`**

```
step 2. Run '/lvmrec.scrpt' to repair the following LVM
 configuration information:
        a. LVM records (lvmrec)
        b. BDRA (Boot Data Reserve Area)
        c. LABEL information

 Requirement:  The following files must reside on disk before
        the script can complete:
        a. /etc/lvmtab
        b. /etc/fstab
        c. /etc/lvmconf/<rootvg>.conf
        d. all device files specified in /etc/fstab
 To run '/lvmrec.scrpt' provide the device filename used to
 access the bootlif as an argument to the script.
 Example:
  /lvmrec.scrpt c0t6d0
  In this example 'c0t6d0' is the device file used to
  access the bootlif.
step 3. Once '/lvmrec.scrpt' completes, issue the command "reboot"
 and bring the system fully up.
 The recovery of the root LVM is complete.  If the '/lvmrec.scrpt'
 issued the following warning:
              "************ I M P O R T A N T ******************"
              "                                                 "
              "Root logical volume has been repaired, but......."
              "you need to reboot the system and repair the Swap"
              "logical volume using the following LVM command:  "
              "   lvlnboot -A n -s /dev/<root lv>/<swap lvol>   "
              "because Recovery has no way to find out what is  "
              "the Swap logical volume information at this point"
              "                                                 "
"*******************************************************"

 The Swap and Dump logical volumes will need to be re-configured.

 The BDRA contains the "root", "swap" and "dump" logical volume
 information.  '/lvmrec.scrpt' only fixes the root logical volume
 information in the BDRA.  The "swap" and "dump" areas can be upda
ted
 via the "lvlnboot" command.

 Example:
    lvlnboot -s /dev/<vg00>/lvol2
    lvlnboot -d /dev/<vg00>/lvol3

  In this example 'lvol2' and 'lvol3' are the "swap" and "dump"
  logical volumes respectively.

step 4. Perform any further data recovery deemed necessary.

*** NOTE ***
  If the same volume group contains more than one corrupted boot d
isk,
  repeat the above steps for each disk that needs to be repaired.
```

This completes the process for installing critical files only.

6336 Paula

Rebuilding the "bootlif" Only

Boot the Core media, following the steps in Chapter 2. You will see some status messages, and then a menu:

```
Welcome to the HP-UX installation process!

    Use the <tab> and/or arrow keys to navigate through the follow
ing menus,
    and use the <return> key to select an item.  If the menu items
 are not
    clear, select the "Help" item for more information.

                          [    Install HP-UX       ]
                          [  Run a Recovery Shell  ]
                          [   Advanced Options     ]
                                  [ Help ]
```

Step 1. Select: **Run a Recovery Shell** . The screen clears, and this is displayed:

```
Would you like to start up networking at this time? [n]
```

Step 2. Enter: **n**

```
* Loading in a shell...
* Loading in the recovery system commands...

(c) Copyright 1983, 1984, 1985, 1986 Hewlett-Packard Co.
(c) Copyright 1979 The Regents of the University of Colorado,
    a body corporate
(c) Copyright 1979, 1980, 1983 The Regents of the
    University of California
(c) Copyright 1980, 1984 AT&T Technologies.  All Rights Reserved.

                  HP-UX SYSTEM RECOVERY CORE MEDIA
                    WARNING:  YOU ARE SUPERUSER !!

NOTE: Commands residing in the RAM-based file system are unsupport
ed 'mini'commands.

These commands are only intended for recovery purposes.

Loading commands needed for recovery!

      WARNING: f ANYTHING is changed on a root(/) that is mirrored
               a 'maintenance mode'(HPUX -lm) boot MUST be done in
                order to force the mirrored disk to be updated!!

     Press <return> to continue.
```

Step 3. Press: **Return**

```
Loading commands needed for recovery!
```

After boot steps, this message appears:

```
 HP-UX CORE MEDIA RECOVERY
   MAIN MENU
 s.  Search for a file
 b.  Reboot
 l.  Load a file
 r.  Recover an unbootable HP-UX system
 x.  Exit to shell
 c.  Instructions on chrooting to a lvm /(root).
Select one of the above:
```

Step 4. To begin the actual system recovery, select: **r**

```
       HP-UX Recovery MENU
 Select one of the following:
a. Mount the root disk and exit to shell only.
b. Recover the bootlif/os partitions.
c. Both options b and c

v. Read information about VxVM/LVM recovery

m. Return to 'HP-UX Recovery Media Main Menu'.
x. Exit to the shell.
```

Step 5. Select **c** to rebuild the bootlif.

```
    BOOTLIF PATH VERIFICATION
       MENU

     This menu must be used to determine the path to the bootlif

 (ISL, HPUX and the AUTO file).
     When the information is correct, select 'a'.

 INFORMATION to verify:
      Path to the bootlif is 56/52.1.0

 Select one of the following:
      a.  The above information is correct.
      b.  WRONG!! The path to bootlif is incorrect.

      m.  Return to the 'HP-UX Recovery MENU.'
      x.  Exit to the shell.

     Selection:
```

6334 Paula

Step 6.

```
BOOT STRING VERIFICATION MENU

        This menu must be used to verify the system's boot string.
        When the information is correct, select 'a'.

    INFORMATION to verify:
         The system's boot string should be:
          'hpux -lm (56/52.5.0)/stand/vmunix'

    Select one of the following:

        a.  The above information is correct.
         b.  WRONG!! Prompt the user for the system's boot string.

         m.  Return to the 'HP-UX Recovery MENU.'
         x.  Exit to the shell.

    NOTE: For an LVM '/'(ROOT) the '-lm' option MUST be specified
   (example: 'hpux -lm (2.3.4)/stand/vmunix' )

    Selection:
```

Assuming that the bootlif path is correct, enter: **a**

Step 7. Assuming the boot string is incorrect, enter **b** at the prompt. You will see a message similar to the following:

```
AUTO FILE should be (replacing 'hpux (56/52.5.0)/stand/vmunix'):
```

Step 8. Enter the correct information (for example, **hpux**); you will then see the BOOT STRING VERIFICATION MENU displayed again:

```
BOOT STRING VERIFICATION MENU

        This menu must be used to verify the system s boot string.
        When the information is correct, select 'a'.

    INFORMATION to verify:
         The system's boot string should be:
          'hpux'

    Select one of the following:
         a.  The above information is correct.
         b.  WRONG!! Prompt the user for the system's boot string.

         m.  Return to the 'HP-UX Recovery MENU.'
         x.  Exit to the shell.

    NOTE: For an LVM '/'(ROOT) the '-lm' option MUST be specified
```

```
        (example: 'hpux -lm (2.3.4)/stand/vmunix' )

  Selection:
```

NOTE

Use the `-lm` option to enter LVM administration mode only when recovering an LVM system.

Use the `-V` option to enter VxVM administration mode only when recovering a VxVM system.

Step 9. Assuming the information is now correct, enter: **a**

- For an LVM system, you will see something like the following:

```
      *********** Installing bootlif  ***********
mkboot -b /dev/rmt/1m  -i ISL -i HPUX /dev/rdsk/c1t1d0
mkboot -a  hpux (56/52.5.0;0)/stand/vmunix /dev/rdsk/c1t1d0
```

```
    RECOVERY COMPLETION MENU
     Use this menu after the recovery process has installed all
requested files on your system.
    Select one of the following:
      a.  REBOOT the target system and continue with recovery.
      b.  Return to the CORWE Media Main Menu.
     Selection:
```

Step 10. Complete the recovery process by selecting a, rebooting your system.

This completes the process for rebuilding the bootlif only.

6332 Paula

Replacing the Kernel Only

Boot the Core media, following the steps in Chapter 2. This menu appears after some status messages:

```
                Welcome to the HP-UX installation process!

    Use the <tab> and/or arrow keys to navigate through the follow
ing menus,and use the <return> key to select an item.  If the menu
 items are not clear, select the "Help" item for more information.

                          [    Install HP-UX       ]
                          [  Run a Recovery Shell  ]
                          [   Advanced Options     ]
                                  [ Help ]
```

Step 1. Click: **Run a Recovery Shell**

```
Would you like to start up networking at this time? [n]
```

Step 2. Enter: **n**

```
* Loading in a shell...
* Loading in the recovery system commands...

HP-UX SYSTEM RECOVERY CORE MEDIA
WWARNING:  YOU ARE SUPERUSER !!

NOTE: Commands residing in the RAM-based file system are
unsupported 'mini' commands. These commands are only intended for
recovery purposes.

Loading commands needed for recovery!

      WARNING:If ANYTHING is changed on a root(/) that is mirrored
               a 'maintenance mode'(HPUX -lm) boot MUST be done in
                order to force the mirrored disk to be updated!!

     Press <return> to continue.
```

Step 3. Press **Return** and the following status message is displayed:

```
Loading commands needed for recovery!
```

Step 4. You will see the following menu:

```
HP-UX CORE MEDIA RECOVERY
   MAIN MENU
 s.  Search for a file
 b.  Reboot
 l.  Load a file
 r.  Recover an unbootable HP-UX system
 x.  Exit to shell
 c.  Instructions on chrooting to a lvm /(root).
This menu is for listing and loading the tools contained
on the CORE media.  Once a tool is loaded, it may be run
from the shell. Some tools require other files to be present
in order to successfully execute.
Select one of the above:
```

Step 5. To begin the actual system recovery, select: **r**

```
 HP-UX Recovery MENU
 Select one of the following:
a. Mount the root disk and exit to shell only.
b. Recover the bootlif/os partitions.
c. Replace the kernel on the root file system.
d. Both options b and c

v. Read information about VxVM/LVM recovery

m. Return to 'HP-UX Recovery Media Main Menu'.
x. Exit to the shell.
```

Step 6. Select **d** to replace only the kernel on the root file system.

```
DEVICE FILE VERIFICATION MENU
   This menu is used to specify the path of the root file system.
   When the information is correct, select 'a'.
 INFORMATION to verify:
       Device file used for '/'(ROOT) is c1t6d0
       The path to disk is 56/52.6.0
 Select one of the following:
      a.  The above information is correct.
      b.  WRONG!! The device file used for '/'(ROOT) is incorrect.
      m.  Return to the 'HP-UX Recovery MENU.'
      x.  Exit to the shell.
```

Step 7. Assuming the root device file is incorrect, select: **b**

```
 Enter the device file associated with the '/'(ROOT) file system
 (example: c1t6d0):
```

On a system with hard-sectored disks, the prompt and response might look like this:

6330 Paula

```
Enter the device file associated with the '/'(ROOT) file system
(For example: c0t1d0s1lvm ) :  device_file
/dev/rdsk/device_file not a special file
<Press return to continue>
Enter the address associated with the '/'(ROOT) file system
(For example: 4.0.1) :  address
  NOTE: if your '/'(ROOT) is not part of a sectioned disk layout
   enter a 'W' for whole disk layout
      or
   enter a 'l' for an LVM disk layout
 instead of a section number.
Enter the section associated with the '/'(ROOT) file system
(For example: 13 ):  13
making rdsk/c0t0d0s13 c 214 0x00000d
making dsk/c0t0d0s13 b 26 0x00000d
```

Step 8. If you were to enter **c1t1d0** as the root device filename.:

```
DEVICE FILE VERIFICATION MENU
  This menu is used to specify the path of the root file system.
  When the information is correct, select 'a'.
INFORMATION to verify:
      Device file used for '/'(ROOT) is c1t1d0
      The path to disk is 56/52.1.0
Select one of the following:
    a.  The above information is correct.
     b.  WRONG!! The device file used for '/'(ROOT) is incorrect.
     m.  Return to the 'HP-UX Recovery MENU.'
     x.  Exit to the shell.
```

Step 9. Since c1t1d0 is the correct root device filename, select: **a**

```
    FILE SYSTEM CHECK MENU
  The file system check '/sbin/fs/hfs/fsck -y /dev/rdsk/c1t1d0'
  will now be run.
Select one of the following:
     a.  Run fsck -y .
     b.  Prompt for the fsck run string on c1t1d0.
     m.  Return to the 'HP-UX Recovery MENU.'
    Selection:
```

M

Step 10. Select **a** to run **fsck -y** to check your file system for corruption; you will see a display similar to the following:

```
** /dev/rdsk/c1t1d0
** Last Mounted on /ROOT
** Phase 1 - Check Blocks and Sizes
** Phase 2 - Check Pathnames
** Phase 3 - Check Connectivity
** Phase 4 - Check Reference Counts
** Phase 5 - Check Cyl groups
6256 files, 0 icont, 149423 used, 1563824 free (928 frags, 195362
blocks)
Mounting c1t1d0 to the CORE media /ROOT directory...
Filesystem      kbytes     used     avail %cap iused  ifree iused Mou
nted on
/ROOT                434773  352461   38834  90% 15241   54647 22%
  ?
Should the existing kernel be
'left', 'overwritten', or 'moved'?[moved]over
```

Step 11. To move the existing kernel with your new file system, enter **move** at the prompt.

Step 12. Complete the recovery process by selecting **a**, REBOOT the target system.

This completes the process for replacing the kernel only.

6328
Paula

System Recovery Questions and Answers

Question: **Can I use a network recovery archive if my system is not network bootable or is not on the same subnet as the Ignite-UX server?**

Yes! One of the new tools developed with the network recovery toolset is `make_boot_tape`, a command that creates a minimal tape that can be used by any client. The tape contains just enough information to boot a client and then connect to the Ignite-UX server where the tape was created. If that is the server where the client's recovery configuration files are stored, the client can then be recovered.

If you initiate recovery archive creation from the Ignite-UX server, the server will warn you if a boot tape is needed for a client. If you ignore this warning, misplace your boot tape, or find that your tape is for the wrong Ignite-UX server, you can always create a new boot tape on the server that you want to use. There is no client-specific information on the tape.

Notice that a tape created by `make_boot_tape` is useful not only for recovery situations, but also for ordinary installations. If you do not want to set up a boot helper for systems not on the same subnet as the Ignite-UX server, you can now simply use `make_boot_tape`.

Question: **What happens if I make changes to a recovery configuration before clicking Go! ?**

In the past, Ignite-UX could not be used to override values in recovery configuration files. Any change made to a recovery configuration from one of the interface screens would result in recovery_mode being turned off, that is, set to false.

This was because Ignite carefully set aside the archive versions of files like */etc/fstab, /etc/mnttab*, and */etc/hosts* when it was running in recovery mode, and restored them after system configuration was complete. If Ignite-UX allowed the user to make changes to file systems, networking, etc. and continue in recovery mode, the files restored from the archive would be out of sync with the reconfigured system.

Beginning with the Ignite-UX A/B 2.0 releases, you can edit values in any of the interface screens without turning off recovery mode. This is possible because critical system files are no longer automatically overlaid by ones from the archive.

Recall that the */etc/fstab* file that Ignite-UX created while configuring the disks was saved to a backup copy prior to extracting the archive. After Ignite-UX boots from the client disk, this fstab is merged with the fstab file extracted from the recovery archive. This merging allows Ignite-UX to preserve information from the old fstab, like entries for file systems not included in the archive, NFS mounts, etc., while accurately representing the configuration changes requested.

Special care needs to be taken when making changes affecting disks not included in the archive. Imagine that you include `vg00` and `vg01` in your recovery archive but not `vg02`. You intend to leave vg02 untouched and simply let Ignite-UX import it for you.

You have also been planning on adding a new disk to the root volume group, and you decide that this is as good a time as any to do it. You choose your recovery configuration from the list and then go to the **Add/Remove Disks** dialogue, where you choose a disk to add. By mistake you choose a disk already in `vg02` instead of your new disk. When your system comes back up, `vg00` and `vg01` are fine, but `vg02` is corrupted.

To avoid scenarios like this, Ignite-UX now "hides" disks intended to be imported again. If you want to see these disks, click the **Additional...** button on the **Basic** tab and change the setting there to show the disks.

Question: **What happens if the pre-install checks fail after I make changes to a recovery configuration?**

In the past if the results of the pre-install checks included one or more ERRORS, Ignite-UX would have to turn off `recovery_mode` to allow users to interact with the user interface and resolve the errors. Unfortunately after the errors were resolved, it was not possible to turn `recovery_mode` back on for the reasons described above.

This created some frustrating situations for users. Imagine that the root disk on a system before it crashes is a 1GB disk with a whole disk layout (not LVM). The only replacement disk available is a 4GB disk. The system administrator therefore uses the 4GB disk, selects the recovery configuration or the system, and gets the following error message from the pre-install checks:

```
ERROR: The selected root disk is too large to use whole-disk
(non-LVM) partitioning. You must either switch to a smaller
root disk, or switch to using LVM to partition the root disk.
```

An experienced Ignite-UX user could do a little handcrafting to configuration files to work around the problem, but a novice user would be stuck.

With the new changes to Ignite-UX, it is no longer necessary to turn `recovery_mode` off when the pre-install checks fail. Now you can simply resolve the problem using the interface and continue running in recovery mode.

Question: **How can I change my setup so that a network recovery archive is available not only on the system for which it was created, but also on other systems with very similar hardware?**

Because networking information can now be changed using the interface and will not be overwritten by files extracted from the archive, it is natural to think about sharing recovery archives for systems with identical or nearly identical hardware. But unlike "global" configurations that appear in the configuration list of all clients, network recovery configurations only appear in the configuration list of the client for which they were created.

The source for shared cfgs is the */var/opt/ignite/INDEX* file that is shipped with Ignite-UX, and the source for client-specific cfgs is the CINDEX file that is created by `make_net_recovery` in the */var/opt/ignite/clients/LLA* directory. One simple way to share a recovery configuration among two systems with similar hardware is to copy the `CINDEX` file and the recovery directory of the client with the archive, to the directory of the client without the archive. The fact that the entries in `CINDEX` use relative paths means that you do not have to change the `CINDEX` file when you copy it. (You may need to export the directory containing the archive to the sharing client.)

Question: **I do not want to interact with the user interface after I reboot the client. How can I have my latest network recovery archive chosen automatically?**

As long as the client is currently booted, use **bootsys -a** to start the install process on the client without the need to interact with the user interface.

Ignite-UX chooses a configuration to use based on these guidelines:

- If */var/opt/ignite/clients/LLA/config* exists, use the cfg specified there.
- If */var/opt/ignite/clients/LLA/config* does not exist, use the default cfg for the client.

The default cfg for the client is the last cfg entry set to true in the CINDEX file if it exists. Otherwise the default cfg is the last cfg set to true in the INDEX file. Because make_net_recovery sets the most recently created recovery cfg to true in CINDEX whenever it creates a new archive, it will be the default unless it is manually changed.

Start Task

To have Ignite-UX choose the latest network recovery archive automatically:

1. Rename or remove the config file currently in the client's directory.
2. Run this from the Ignite-UX server:

```
bootsys -a client
```

Question: **Why does ioscan core dump when running make_tape_recovery or make_net_recovery?**

It is possible for ioscan to core dump due to the value set for the COLUMNS environment variable in versions prior to HP-UX 11i. When the -n option is used ioscan uses the COLUMNS variable to determine how wide the screen is when formatting the names of device files. If a core dump occurs, you will see messages similar to these:

```
sh: 13061 Floating exception(coredump)
WARNING: pclose of ioscan returned: 34816
```

6324

Should this happen, unset COLUMNS then rerun make_tape_recovery or make_net_recovery. If you are using an xterm, hpterm, or dtterm to run make_tape_recovery or make_net_recovery, do not resize the terminal window to a smaller size instead minimize it if is in the way.

Question:

Can I run make_net_recovery from a PA server to create an archive for an IPF client or vice versa?

Yes, this is possible though additional steps must be taken. Although the B.4.0 or later versions of Ignite-UX can be installed on both IPF and PA systems, make_net_recovery command cannot automatically swpackage the network recovery tools into /var/opt/ignite/depots/recovery_cmds depot for a client with mismatched hardware architecture.

For example, a server is an IPF system with the B.4.0 version of Ignite-UX installed and is being used for PA clients. When make_net_recovery is run from the GUI to create a recovery archive of a particular PA client, an error similar to this appears:

```
Error Message: Swinstall(1M) failed to install recovery tools from
: "funhouse: /var/opt/ignite/depots/recovery_cmds"
```

To work around this issue, you have to execute the following steps manually:

1. Run /opt/ignite/lbin/pkg_rec_depot command to generate the IUX-Recovery bundle in /var/opt/ignite/depots/recovery_cmds on the IPF server:

   ```
   /opt/ignite/lbin/pkg_rec_depot
   ```

2. Run swcopy the entire Ignite-UX product with the right architecture for the client.

   ```
   swcopy -x layout_version=0.8 -s /[depot path] B5725AA @ \
   /var/opt/ignite/depots/recovery_cmds
   ```

3. Ensure that the correct bundles are now in

   /var/opt/ignite/depots/recovery_cmds, by entering:

   ```
   swlist -l bundle -s /var/opt/ignite/depots/recovery_cmds
   ```

   Messages similar to the following should appear:

   ```
   # Initializing...
   ```

```
# Contacting target "funhouse"...
#
# Target:  funhouse:/var/opt/ignite/depots/recovery_cmds
#


B5725AA                 B.4.0.203      HP-UX Installation
Utilities    (Ignite-UX)


IUX-Recovery            B.4.0.203      Ignite-UX network
recovery tool subset

Ignite-IA-11-22         B.4.0.203      HP-UX Installation
Utilities for

Installing 11.22 IA Systems

Ignite-UX-10-20         B.4.0.203      HP-UX Installation
Utilities for

Installing 10.20  Systems

Ignite-UX-11-00         B.4.0.203      HP-UX Installation
Utilities for

Installing 11.00  Systems

Ignite-UX-11-11         B.4.0.203      HP-UX Installation
Utilities for

Installing 11.11  Systems
```

4. Re-launch Ignite-UX, enter:

   `ignite`

Now, you can create archives for different hardware architectures from this IPF server. The same steps can be used on PA servers to accomplish the same thing.

A Troubleshooting

Likely problem areas described in this appendix are:

- Errors and Warnings.
- Ignite-UX Server Problems.
- Installing Systems with Ignite-UX.
- Installing from Media.
- Installing from Archives (golden images).
- Running swinstall.
- Adjusting File System Size.
- Troubleshooting Large Systems.
- Media Recovery.
- Network Recovery.

This appendix includes troubleshooting hints from the Ignite-UX FAQ. For the latest on Ignite-UX problems and workarounds, see the Ignite-UX FAQ:

`http://www.software.hp.com/products/IUX/faq.html`

To receive the most-recent FAQ via email, send an empty message (no subject or content required) to:

`iux_faq@igniteux.fc.hp.com`

6320 Paula

Errors and Warnings

As an HP-UX install progresses, you will see messages relating to the progress being entered into the log file. Usually these messages are related to normal behavior. `ERROR` and `WARNING` messages have the following significance:

`ERROR` This indicates a serious problem, usually requiring action from the user in order to proceed with an installation.

`WARNING` This indicates something out of the ordinary, but *not* fatal. The warning *may* require action.

If you see a message, or experience unusual behavior, you can use the following sections as prioritized lists of likely problems and their solutions. They are grouped by the following topics, with the problems you are most likely to encounter near the beginning of each section.

Ignite-UX Server Problems

GUI core dumps

Ignite-UX GUI core dumps.

If your system has patch PHSS_12824 (Motif), remove it or install PHSS_13743. Patch PHSS_12824 was found to be bad.

Mixed versions of Ignite-UX

Can't find `/d_cfg_mnt_sb61/monitor_bpr` ***after updating the server.***

This is caused by having a mix of Ignite-UX fileset revisions on your server. In most cases it happens when you update only one release bundle (like Ignite-UX 10.20) even though you install other releases from that server.

An easy way to check for this case is to look at the output from the command:

```
swlist Ignite-UX
```

All the filesets should have the same revision, if not then you need to install all consistent versions. If you have **boot-helper** systems (see Appendix B), they also need to have the Ignite-UX product updated to match the same revision as the server that they reference.

Cannot determine dump size limit

Ignite-UX servers "Cannot determine dump size limit."

If you have a saved client config created using a version of Ignite-UX prior to 1.51, and then update Ignite-UX to 1.51 or later, and if you initiate the install from the Ignite-UX server GUI, it will give an ERROR looking something like this:

```
ERROR: Unable to determine dump size limit for disk (8/4.8.0),
release (B.10.20). Internal Ignite-UX error.
```

The problem is that an old version of the clients' `hw.info` file is being examined by the new Ignite-UX. To fix things, merely boot up the client system using:

```
boot lan.IP install
```

or whatever syntax your system supports from the boot prompt. *IP* is the IP address of your Ignite-UX server. The client `hw.info` file will be updated, and everything should proceed normally.

Installing Systems with Ignite-UX

Installs stop after 30 INDEXes

Installs are broken after 30 INDEX entries.

A modification was made to the **Basic** tab in Ignite-UX 1.42 so that if the `INDEX` file has more than 30 configurations (18 in the terminal user interface), then a list with scrolling is used. For example:

```
[Configurations:...] HP-UX B.11.00 Default [Description...]
```

One of the side effects of this is that sometimes a chosen configuration from a large list doesn't get parsed correctly.

Either update to the current Ignite-UX version or make sure that the text name for each configuration (when there are more than 30) is 25 characters or less. Then the chosen configuration will be correctly parsed. For example, this config name:

```
cfg "HP-UX B.10.10 long configuration name" {
description "long configuration name."
"/opt/ignite/data/Rel_B.10.10/config"
"/var/opt/ignite/config.local"
}
```

has a configuration of 37 characters, `"HP-UX B.10.10 long configuration name"`

and will not be correctly parsed. Shortening this will solve the problem:

```
cfg "HP-UX B.10.10 l.c.n." {
```

Another work-around is to use 30 configurations at most.

samreg errors

Igniting from an archive returns numerous "samreg" errors.

The problem is that the SAM filesets haven't been configured when certain products are trying to register themselves with sam. The workaround is to place the following config stanza in `/var/opt/ignite/config.local` or directly in the config file with the "core" sw_source:

```
sw_source "core"
{
post_load_cmd += "

swconfig -xautoselect_dependencies=false
-xenforce_dependencies=false SystemAdmin.SAM "
}
```

Problem installing clients on multiple subnets

Problems installing clients on multiple subnets.

There are a couple of problems with having an Ignite-UX server that is multi-homed (connected to multiple subnets):

- The `instl_bootd` daemon allocates IP addresses from the `instl_boottab` file without knowing which IP addresses are valid for the subnet that the client is requesting to boot from. Due to this lack of information, it can allocate an IP address that is not valid for the client's subnet, and thus the client will not be able to boot from the server.

  The workarounds for this problem are:

  - For every possible client that you may want to boot, assign "reserved" IP addresses in `/etc/opt/ignite/instl_boottab` that are tied to the client's LLA address. This will ensure that `instl_bootd` will allocate an appropriate address (See the comments in the `instl_boottab` file on how to reserve addresses). Alternatively, you can set up entries in `/etc/bootptab`.
  - Configure a boot-helper system on each subnet that the client can boot from before contacting your central Ignite-UX server. See Appendix C.

- The "server" keyword that specifies the IP address for your Ignite-UX server can only correspond to one of the LAN interfaces. If each subnet is routed such that all clients can use the one IP address to contact their server, then the install will work.. However, it is more efficient for the client to use the server's IP address that is connected

6.3b ✓

directly to the client's own subnet. If a client is on a subnet that does not have a route to the IP address specified by "server", then it will not be able to contact the server after it boots.

Workarounds for this problem are:

- Manually correct the server's IP address on the networking screen that appears on the client console when you boot the client.
- Use a boot-helper on each subnet. When using a boot-helper, the server's IP address can be specified correctly on each helper system.

Too much file space needed

Ignite-UX needs more file system space than expected.

Ignite-UX adds in minfree (normally 10%) to the amount required by the software impact. You may have software bundles that have overlapping contents (filesets and/or files). `make_config` makes `sw_impact` statements for each bundle without doing anything special to guard against over-counting when the bundles overlap. For example the Ignite-UX-10-*xx* bundles all overlap quite a bit, so that when you load all of them via Ignite-UX, it estimates too much space. To find the space needed, add the `sw_impact` of all the `sw_sels` that you are loading.

Debugging SD during cold install

How do I monitor SD operation during cold installs from the Ignite-UX server?

The first level debug of SD produces copious output. Because the logs are captured on the servers as well as the client this would run Ignite servers out of disk space rapidly if every install had this turned on.

It is fairly straight forward to do this on a per-session basis without modifying the config files. From the initial Ignite-UX menu, select: **Advanced Options -> Edit config file** This will run vi and you could add, for example:

```
env_vars += "SDU_DEBUG_RPC=1"

sd_command_line += " -x logdetail=true -x loglevel=2
```

Booting older workstations

An HP 9000 715/50 workstation won't network boot off of the Ignite-UX server.

Older Series 700 workstations require `rbootd` running on the server. If the server is FDDI, `rbootd` won't run. In that case boot from media then switch the source to the Ignite-UX server. Older ones use RMP not BOOTP and require rbootd to translate and hand off to `bootpd`.

RMP clients are the older Series 700 workstations: 705, 710, 715, 720, 725, 730, 735, 750, 755.

BOOTP clients are the Model 712 and future workstations, as well as K-Class, D-Class and newer Series 800 servers.

Booting errors

Error: `IPL error: bad LIF magic`

Possible problems are:

- Not having tftp access to `/opt/ignite` and `/var/opt/ignite`, the `/etc/inetd.conf` file on the server should have an entry such as:

  ```
  tftp dgram  udp wait   root /usr/lbin/tftpd    tftpd\
  /opt/ignite\
  /var/opt/ignite
  ```

  If not, fix `inetd.conf` and run **`inetd -c`**. Kill any `tftpd` processes that may be running. Loading Ignite-UX should set up inetd.conf. If not, check SAM.

- Using a bootptab entry for the client that is referencing a non-existent boot file (bf).
- A corrupted `/opt/ignite/boot/boot_lif` file.
- Perhaps some remnants of the old cold-install product (NetInstall) conflicting with Ignite-UX (old `instl_bootd` running)
- A defect in the `rbootd` daemon delivered in patch PHNE_10139. If you have this patch loaded and do not need it for DTC devices, try removing it or updating to patch PHNE_11017 (10.20) or PHNE_11016 (10.10).

Booting on IPF with /etc/bootptab error

Error: ***`PXE-E16: Valid PXE offer not received.`***

`Exit status code: Invalid Parameter`

When using `/etc/bootptab` to define Ignite-UX boot servers, a number of problems can be introduced resulting in this error. The following checklist can be used to isolate the problem:

1. Check `inetd`
   - Check `/etc/inetd.conf` to make certain `bootps` and `tftp` entries have been uncommented. Make certain the `tftp` line contains `/opt/ignite` and `/var/opt/ignite` paths on the `tftp` line.
   - Check to see if `inetd` was restarted or given an option to re-read the configuration files (`inetd -c`), after the files were edited? Is the `inetd` process running?
   - Check for entries in /`var/adm/inetd.sec` that may cause `inetd` to deny service to certain clients.
   - Check `/var/adm/syslog/syslog.log` to make certain `inetd` was restarted, and that no bad messages are found.
   - Check for messages from `bootpd` and `tftpd`.
2. `Check bootpd`
   - Check the `/etc/bootptab` entry. Make certain the MAC address matches the client MAC address. Use `dhcptools -v` to validate the format of the `/etc/bootptab` file.
   - Check for entries in `/etc/dhcpdeny` to insure that `bootpd` is not set to deny service for particular clients.
   - Check `/var/adm/syslog/syslog.log` for a message from `bootpd` that indicates it was started when a `bootpd` packet was received.

     If packets were not received, use a tool such as `tcpdump` to check for network packets. Verify that `bootp` packets are being seen by the system.
   - Check to see if there are other systems on the network that may also be replying to the booting client system.

- Check to see if the system booting is on a different subnet to the bootp server ensure that any router between the two allows the forwarding of bootp requests (Note that the configuration is router specific.).

3. Check tftpd

   - Check the tftp line in /etc/inetd.conf to make certain /opt/ignite and /var/opt/ignite directories are listed.
   - Check the tftpd connection manually by using the tftp command, for example:

```
a.  $ tftp [server-name]
b.  tftp> get /opt/ignite/boot/nbp.efi /tmp/nbp.efi
    Received [n] bytes in [s] seconds
c.  tftp> quit
```

Problems pointing to client over network

I put control_from_server=true and run_ui=false in the INSTALLFS, but I still get prompted for information on the client.

Possible problems are:

- If the screen is showing the client name in an editable field and a cancel button at the bottom of the screen, then all is well and there should be an icon waiting for you on the Ignite-UX screen. The text screen allows you to change the icon name, or switch to a client side install.
- If the screen is showing two or more lan interfaces to select from, then there wasn't enough information in the config files to tell it which LAN to use. Once you select a LAN and select **Install HP-UX**, you should be set.
- If the screen is prompting you for networking information, then either DHCP didn't respond or there isn't an entry in /etc/bootptab for the client. Enter the network information, select **Install HP-UX** and continue the install.

Mount errors when igniting 10.20 systems

Errors regarding mounting a file system occur when igniting 10.20 systems.

Patch PHCO_18317 supplies a new version of /sbin/mount but is not compatible with Ignite-UX. If this patch is loaded via either an archive or SD, then the next swinstall session will have fatal errors that appear like this

```
ERROR:   "c02380:/":  One or more filesystems that appear in the
filesystem table are not mounted and cannot be mounted.
ERROR:   Entry for filesystem "/dev/vg00/lvol1" in "/etc/fstab"
could
not be mounted.  If you do not want this file system mounted,
comment it out of the "/etc/fstab" file, or set the
"mount_all_filesystems" option to "false".
ERROR:   Cannot continue the Analysis Phase until the previous
errors
are corrected.
```

One workaround is to add the following to your configuration:

```
sd_command_line += " -xmount_all_filesystems=false "
```

However this has the unpleasant side effect that each swinstall session produces a warning message stating that file systems will not be mounted.

Patch PHCO_19694 replaces PHCO_18317. Note that recovery methods are unaffected because they are solely OS archives, and no SD activity takes place.

Applications hang after igniting

Some applications and shells hang over NFS after igniting.

The reason for the hang is most likely due to a problem with the NFS file locking daemons rpc.statd and rpc.lockd caused by the action of reinstalling the system. Many applications use file locking and can hang in this situation. Most common is user home directories that are NFS mounted, in which case sh and ksh will attempt to lock the .sh_history file and hang before giving the user a prompt.

When a system is running and has an active NFS mount with a server in which files have been previously locked, both the client and server cache information about each other. Part of the information that is cached is what RPC port number to use to contact the rpc.lockd daemon on the server and client.

This RPC port information is cached in memory of the running rpc.statd/rpc.lockd process on both the server and client sides. The rpc.statd process keeps a file in the directory /var/statmon/sm for each system that it knows it should contact in the event that the system reboots (or `rpc.statd`/`rpc.lockd` restarts). During a normal reboot or crash, `rpc.statd` will contact each system in `/var/statmon/sm` and inform them to flush their cache regarding this client.

When you re-install a system, the `/var/statmon/sm` directory is wiped out. In this case, if the reinstalled system tries to re-contact a server that has cached information, the server will try to communicate over a old RPC port. The communication will fail for `rpc.lockd` and any file locking done by an application over that NFS mount will hang.

There are a several ways to avoid and/or fix the problem if it happens:

- If you are using `bootsys` to install clients, use the `-s` option to allow the client to shutdown normally and thus inform servers that it is going down.
- If you experience a hang, you can reboot the client, or kill/restart `rpc.lockd` and `rpc.statd` on the client. At the point of the hang, the `/var/statmon/sm` directory will contain the name of the server, and thus rebooting or restarting the daemons will tell the server to flush it's cache. If more than one server is involved you may end up doing this multiple times until all servers are notified.
- As part of the installation, create a file for each server in `/var/statmon/sm` which contains the server's name. This will cause the first boot to generate a crash recovery notification message to each server, causing them to purge the stale port information. Below is an example `post_config_cmd` that could be placed in your `/var/opt/ignite/config.local` file. Replace `sys*` with your NFS server names.

```
post_config_cmd += "
   mkdir -p /var/statmon/sm
   for server in sys1 sys2 sys3
   do
      echo $server > /var/statmon/sm/$server
      chmod 0200 /var/statmon/sm/$server
   done
"
```

bootsys seems to work in reverse

With* `bootsys -w client`*, the client doesn't wait for the server. With* `bootsys client`*, the client waits for the server.

This was probably due to your running through the UI once on the server prior to running bootsys. The server drops the instruction for the client to start installing and the next time the client boots it picks that up and goes. Ignite-UX tells you that the install will happen the next time that `bootsys -w` is used, but does not really say it will happen automatically. And, the next time you did a bootsys, you had not used the UI without the client being booted from the server.

Booting diskless clients

bootsys does not work on diskless clients.

bootsys does not support rebooting HP-UX 9.x and 10.x diskless clients from the Ignite-UX server.

If you need to remotely reboot diskless clients from the Ignite-UX server, follow these steps:

1. If you need to duplicate the behavior of the `-w` or `-a` options to bootsys, you will need to modify the INSTALLFS file using instl_adm to set the keywords `run_ui` and/or `control_from_sever` appropriately. Or you can do this using Ignite-UX under the **Options -> Server Configuration** menu (Run client installation UI option).
2. Copy the `/opt/ignite/boot` directory and contents to the diskless server as `/opt/ignite/boot`:

   ```
   rcp -r /opt/ignite/boot  diskless-server:/opt/ignite/boot
   ```

3. Edit the client's entry in /etc/bootptab on the diskless server to set the `bf` (boot file) flag to be `/opt/ignite/boot/boot_lif`:

   ```
   bf=/opt/ignite/boot/boot_lif
   ```

   You may also need to set the bootptab entries for the gateway (gw), and subnet-mask (sm). The networking information in the bootptab file will satisfy the client's DHCP request for networking information when it boots. So it will need everything required to contact the Ignite-UX server.

4. Run `setup_tftp` on the diskless server to allow tftp access to `/opt/ignite`:

   ```
   /usr/sam/bin/setup_tftp /opt/ignite # on 9.X systems

   /usr/sbin/setup_tftp /opt/ignite # on 10.X systems
   ```

5. With this setup, the next time you reboot the client from the diskless server it will load the INSTALL kernel and INSTALLFS file system from the diskless server. The client will then contact the Ignite-UX server and the installation can proceed as usual.

Server not listed

`search lan install` doesn't list the server.

Check these items on the Ignite-UX server from which you are trying to boot:

- Messages from `instl_bootd` in `/var/adm/syslog/syslog.log`. If you need to add more IP addresses to `/etc/opt/ignite/instl_boottab` you will see messages in `syslog.log` such as the following:

  ```
  instl_bootd: Denying boot request for host: 080009F252B3 to
  avoid IP address collision. Try booting again in 214 seconds, or
  add more IP addresses to /etc/opt/ignite/instl_boottab.
  ```

- A message in syslog.log that indicates that you have no IP addresses in */etc/opt/ignite/instl_boottab* is:

  ```
  instl_bootd: No available IP address found in:
  /etc/opt/ignite/instl_boottab
  ```

- If the client is an older system that does not use the `BOOTP` protocol (like 720s, 710s, 735s, 750s) then also look in the log file `/var/adm/rbootd.log`, and check to make sure that the rbootd daemon is running. rbootd always runs, where as `instl_bootd` is started via `inetd` and only runs when needed.

  Also, for these older clients, there is an intentional delay built into the rbootd process when a client wants to do an install boot (as opposed to a diskless boot). This prevents the server from showing up during the first search. Retrying the search two or three times may be necessary.

bootsys fails with insufficient space

bootsys fails due to insufficient space in the `/stand` volume

bootsys needs to copy the two files: `/opt/ignite/boot/INSTALL` and `/opt/ignite/boot/INSTALLFS` from the server into the client's `/stand` directory. This error indicates that there is not enough space in /stand. To fix this, you may need to remove any backup kernels. Also check for kernels in the `/stand/build/` directory (like `vmunix_test`).

6-308

bootsys failure

bootsys -i configuration [sys1...] fails.

A defect in Ignite-UX A/B.2.2 releases prevents bootsys from successfully pushing a specific configuration out to a client. To fix this:

1. Enter: **vi /opt/ignite/bin/bootsys**
2. Move to line 848 in the file:

   ```
   if [[ "c_opt" != "$PUSH_MODE" ]]; then
   ```

3. Change c_opt to $c_opt and save the change. bootsys will now work correctly.

This defect will be fixed in the Ignite-UX A/B 2.3 release.

Installing from Media

DCE/RPC errors

DCE / RPC errors (RPC exceptions) occur during the configuration stage, plus a failure message is printed at the end of the installation.

There is an apparent problem with certain SD operations (for example, `swacl`) when only loopback networking is enabled. This would occur if the "media only" installation option is selected. The workaround is to install using the "media with networking enabled" option and set up (perhaps temporary) networking parameters: hostname, IP address, netmask, routing, etc. SD operations will complete normally.

Patch installation hangs

swinstall hangs during patch software analysis.

If you have created a CD-ROM that uses depots containing patches and the swinstall command that is loading the patches hangs, then you may be running into a defect in the `df` command.

To be sure, type `^C^C^C` until you get a prompt asking if you want to stop the install. Answer **yes**, then answer **yes** to push a debug shell. From the shell, run `ps -ef` and look for a hung `df` command.

The problem is caused by a defect in the df command. The defect is that it hangs whenever it sees a mount entry with a one-character device string (in this case the mount device is "/").

The workarounds for this problem are:

- If the core OS is loaded from an archive, make sure that the latest `df` command patch is part of that archive (PHCO_15344 or its successor)

6.308

- If the core OS and patches are both in the same depot, and you are using the hw_patches_cfg config file to cause loading of the patches, then add the following to your config file:

```
sw_source "core patches" {
   pre_load_cmd += "
      sed '/^. /d' /etc/mnttab > /tmp/mnt.fix &&
      cp /tmp/mnt.fix /etc/mnttab
      rm -f /tmp/mnt.fix
   "
}
```

- Install the latest version of Ignite-UX.

Installing from Archives (golden images)

Can't find specified archive

```
Errors: gunzip: stdin: unexpected end of file
        pax_iux: The archive is empty.
ERROR: Cannot load OS archive (HP-UX Core Operating System
Archives)
```

The NFS mount probably succeeded, but the file was not accessible from the target machine. Check these possibilities:

- File has a different name (check your config files).
- File has the wrong permissions such that it is not readable (check /etc/exports).

Missing .conf files

/etc/nsswitch.conf and /etc/resolv.conf files from the archive don't end up on the install target.

Ignite-UX changes some files during the configuration process, including resolv.conf and nsswitch.conf. Ignite-UX's os_arch_post_l and os_arch_post_c scripts place these files on the target system after the install.

These scripts are delivered in /opt/ignite/data/scripts/. You will probably only need to modify os_arch_post_l. Search on resolv.conf and nsswitch.conf for directions on what to change. After the script has been changed, modify your config file which describes the archive to point to the new script.

pax_iux errors

```
pax_iux: X: Cross-device link
pax_iux: X: File exists
```

Both of these errors may occur when loading a system from an archive that does not have the same file-system partitioning as the system from which the archive was created.

The Cross-device link error is caused when two files exist as hard links in the archive, and when the two files would end up in separate file-systems. For example, if you created an archive on a system that did not use LVM, in which case the root file system is all one file system. And, say you have two files: /usr/local/bin/f1 and /opt/myprod/bin/f2 are hard links. This error will occur if you make an archive of this system and try to apply it to a system that uses LVM and has /usr and /opt as separate file systems.

The File exists error may occur when the archive has a symlink, or regular file, that is named the same as a directory or mount point that exists when the archive is loaded. This may happen for example if the original system that the archive was made from has a symlink like */opt/myprod* -> */extra/space*. And then when you are loading a system from the archive you decide to create a mounted file system as /opt/myprod. The pax command will fail to create the symlink because a directory exists in it's place.

When the error happens you will be asked if you want to push a shell (on the target's console). Answer **yes**, and from the shell, enter **exit 2** to ignore the error and it will continue on. Once the system is up, you can more-easily determine what should be done with the paths it complained about.

To avoid the error, the system that the archive is created from should not contain hard links between directories that are likely to be created as separate file systems.

Running swinstall

Tape not readable

swinstall cannot read the tape. For example you may see:

```
Source connection failed for "ignitesvr:/dev/rmt/0m".
```

Possible causes and fixes are:

- Wrong device file — Use the **Actions** menu in SAM's **Peripheral Devices/Tape Devices** area to show the device files for the tape drive.
- Failure reading the contents of the tape:
  - No device file present for the tape — Use the **Actions** menu in SAM's **Peripheral Devices/Tape Devices** area to create the device files for the tape drive.
  - Bad/wrong tape — Verify label on tape. Check the contents. SD tapes are in tar format:

    ```
    tar tvf device_file | more
    ```

    For example, if the tape device is `/dev/rmt/0m`, enter:

    ```
    tar tvf /dev/rmt/0m | more
    ```

    You should see a tar format table of contents. If you do not see this, the tape is corrupt.
  - Dirty head in DDS tape drive — Use a DDS tape cleaning cartridge to clean the tape head.

Adjusting File System Size

The absolute minimum /usr file-system sizes needed to update to HP-UX 11.0 are:

- For 32-bit: 300 MB.
- For 64-bit: 324 MB.

If the required file-system size for the bundle you copy to a depot exceeds that file system limit set by your disk installation, you will get an error condition during the copy process. Use lvextend and extendfs in this situation to create a larger file system. You might have a problem updating your system(s) if the /usr or /var volume is too small.

If you try an update, swcopy determines how much disk space is required. If there isn't sufficient space, swcopy reports an error:

```
ERROR: The used disk space on filesystem "/var" is estimated
to increase by 57977 Kb.
This operation will exceed the minimum free space for this
volume.  You should free up at least 10854 Kb to avoid
installing beyond this threshold of available user disk space.
```

In this example, you would need to increase the file system size of /var by 10 MB, which actually needs to be rounded up to 12 MB.

Follow these steps to increase the size limit of /var:

Step 1. Determine if any space is available by entering:

```
/sbin/vgdisplay
```

You should see a display like this:

```
         - Volume groups -
VG Name                     /dev/vg00
VG Write Access             read/write
VG Status                   available
Max LV                      255
Cur LV                      8
Open LV                     8
Max PV                      16
Cur PV                      1
Act PV                      1
Max PE per PV               2000
VGDA                        2
PE Size (Mbytes)            4
```

```
Total PE                      249
Alloc PE                      170
Free PE                       79
Total PVG                          0
```

Free PE indicates the number of 4MB extents available, in this case this is 79 (equivalent to 316 MB).

Step 2. Shutdown the system: **`/sbin/shutdown`**

Change to single user state. This will allow `/var` to be unmounted.

Step 3. Enter: **`/sbin/mount`**

You will see a display similar to this:

```
/ on /dev/vg00/lvol1 defaults on Sat Mar 8 23:19:19 1997
/var on /dev/vg00/lvol7 defaults on Sat Mar 8 23:19:28 1997
```

Step 4. Determine which logical volume maps to */var*. In this example, it is `/dev/vg00/lvol7`.

Step 5. Enter: **`/sbin/umount /var`**

This is required for the next step, since extendfs can only work on unmounted volumes.

Step 6. Extend the size of the logical volume:

```
/sbin/lvextend -L new_size_in_MB /dev/vg00/lvol7
```

For example, this makes the volume 332 MB:

```
/sbin/lvextend -L 332 /dev/vg00/lvol7
```

Step 7. Extend the file system size to the logical volume size:

```
/sbin/extendfs /dev/vg00/rlvol7
```

Step 8. Enter: **`/sbin/mount /var`**

Step 9. Either go back to the regular init state,`init 3` *or*`init 4`, or reboot.

6.300

Troubleshooting Large Systems

During system analysis

On a large system such as a T500 with a very large number of disk drives (such as 50 or more), you may see messages such as these during the system analysis phase of cold install:

```
Out of inode- can't link or find disk
or
Write failed, file system is full.
or
File system full.
```

To reduce the likelihood of this problem occurring, before you do the installation you should *turn off any disks you don't plan to use for the installation process and start over.*

After the system is cold-installed, you may wish to add back all the file systems that existed under the previous installation, either manually or using SAM. However, for a large number of file systems (for example, over a hundred), some tables in the kernel may be too small to allow correct booting. This is because the newly-installed kernel contains default values for kernel table sizes, and does not allow for special configurations made to the kernel installed previously.

For example, the first boot after adding the file systems may result in error messages displayed to the console, such as the following:

```
inode: table is full
proc: table is full
file: table is full
```

Boot failures

The boot may fail in various ways. You may be have to do file system repair manually. If this is not possible, the kernel may need to be re-configured before booting. The following settings should allow the kernel to be booted, but may not be optimal for the system:

```
ninode = 2048 (default is 476)
nproc = 1024 (default is 276)
nfile = 2048 (default is 790)
```

Alternatively, you can re-configure the kernel by either raising `maxusers` to a large value, such as `200`, or selecting an appropriate bundle of SAM-tuned parameters from the SAM **Kernel Configuration Actions** menu. Be sure to determine the correct configuration for your system.

Media Recovery

tftp access

When running the recovery system option from a client booted in Ignite-UX, errors seem to point to files not being accessible via tftp.

Only /opt/ignite and /var/opt/ignite should be needed for tftp access.

make_sys_image broken

Level 2 make_sys_image is broken at version 1.51.

Yes, but there is a quick fix:

Change line 1303 of /opt/ignite/data/scripts edit make_sys_image from:

```
if [[ ${recovery_mode} != "TRUE" ]]; then
```

to:

```
if [[ ${recovery_mode} = "TRUE" ]]; then
```

Hot-swapping disks

Problems hot swapping disks during recovery.

Ignite-UX supports only hot swappable disks that are completely installed, and not removed when creating a recovery image. Proper software and hardware procedures must be used for hot swap disk removal or replacement before or after recovery, but not in the middle. The LVM command lvlnboot used by save_config does not work when a disk is removed and the system is in this odd state. If this command is not working, then make_recovery has no chance of succeeding.

Volume group error

Error: `The minor number of the volume group exceeds the value IUX can support.`

The make_net_recovery command check to ensure that it does not back up a system that Ignite-UX will be unable to recreate.

Ignite-UX version A.*x.x* can only create volume groups with group numbers in the range 0 to 10. This is due to the *maxvgs* kernel tunable being set to 10 in the INSTALL kernel. In order to continue to have Ignite-UX work on systems with 32 MB of memory, the kernel cannot have this parameter increased.

Ignite-UX B.*x.x* does not have this restriction due to reductions in the amount of memory LVM consumes.

`make_net_recovery` can operate on non-root volume groups so it is not uncommon to see the error with this tool.

Possible workarounds:

- If you got into this situation by manually recreating the LVM device files, then consider renumbering them to something less than 10.
- If using `make_net_recovery`, exclude that volume group from the archive.
- Use Ignite-UX B.*x.x* on HP-UX 11.0/11i systems.

`vgcreate` error

vgcreate error during recovery of a 9GB disk.

If you used Ignite-UX 1.48 or 1.49 to create a recovery tape of a system with a 9GB disk, you may experience a failure when you try to use this tape. The failure would result in the message similar to the following:

```
* Creating volume group "vg00".
vgcreate: Not enough physical extents per physical volume.
Need: 2170, Have: 2169.
ERROR:   Command "/sbin/vgcreate -A n -e 2169 -l 255 -p 16 -s 4
/dev/vg00 /dev/dsk/c1t15d0" failed.

The configuration process has incurred an error, would you like to
push a shell for debugging purposes? [y/n]
```

Either update to the latest Ignite-UX release and recreate the tape, or work around the problem when it happens. To work around the problem, answer **yes** to push a shell. From this shell, enter the command as shown in the error you get, but add 1 to the value shown for the `-e` option. When you successfully run `vgcreate`, enter **`exit 2`** from the shell to continue the install.

Online diagnostics not restored

Online Diagnostics LIF files are not restored during a recovery.

Ignite-UX destroys the old LIF area on the boot disk and lays down new LIF volumes every time the system is installed. At no point during the installation are the old LIF volumes copied and restored to the disk.

To restore the LIF volumes to the disk, reinstall the application, or look at the SD configure scripts for the application and rerun the commands which put the LIF volumes in place on the disk. For example, for the OnlineDiag bundle, the /var/adm/sw/products/LIF-LOAD/LIF-LOAD-MIN/postinstall script puts the OnlineDiag LIF volumes onto the root disk. It uses this command:

```
/usr/sbin/diag/lif/lifload -f /usr/sbin/diag/lif/updatediaglif
```

Bad IPL checksum error

"bad IPL checksum" error when booting B1000, C3000, and J5000.

The 1.8 revision of firmware on the B1000, C3000, and J5000 workstations has a defect that causes them to give a "bad IPL checksum" error when booting from a make_recovery tape (and possibly other bootable tapes as well).

If you have one of these systems, your options are to update the system firmware once a new version with a fix is made available, or to use Ignite-UX version A/B.2.0 or later which works around the problem.

Network Recovery

Failure when archiving large volumes

make_net_recovery fails when the archive is 2GB or more.

make_net_recovery uses NFS to write/read the system archive from the client to/from the server. To manage archives greater than 2GB requires that both the client and server use NFS protocol version 3 (PV3). NFS PV3 is available for HP-UX 10.20 when the Networking ACE set of patches are loaded, and is standard on HP-UX 11.0.

If you know you have NFS PV3 and are having problems, check:

- You must be running Ignite-UX version A.2.1(on HP-UX 10.*x*) or later, or B.2.0 (on HP-UX 11.*x*) or later.
- Some NFS patches in the past have caused problems with >2GB files. These problems have been fixed in patches:

  ```
  10.20: PHNE_17619 (S700), PHNE_17620 (S800)
  11.00: PHNE_17247
  ```

- If your NFS server is running HP-UX 10.20 with the newer NFS patches, then the /etc/rc.config.d/nfsconf file has a configurable parameter (MOUNTD_VER) which determines if the default mount should be PV2 or PV3. This must be set to 3.

  If your clients are running HP-UX 10.20 with the newer NFS patches, the /etc/rc.config.d/nfsconf file must have the parameter MOUNT_VER set to 3.

Volume groups erased

make_net_recovery version 2.0 erases volume groups that contain only unmounted and raw logical volumes.

make_net_recovery version 2.0 has a bug which causes volume groups that contain only unmounted and raw logical volumes to be re-created but not restored, causing loss of data. When recovering a system, the user can specify to not recreate these volume groups, so that data is not lost. However, the user will need to manually import these volume groups after recovery. This problem has been fixed with version 2.1.

Core dumps

make_net_recovery version 2.0 and 2.1 core dumps when archiving more than 8 volume groups.

This problem is fixed with Ignite-UX 2.2.

Problem with NFS mounts

`make_net_recovery` version 2.0 and 2.1 crosses and archives NFS mounts if an essential directory has a symbolic link to something that is NFS mounted, and the path to the NFS mounted directory contains a directory which is a symlink.

This problem is fixed with version 2.2.

LAN address changes

After replacing the client system, the LAN address is now different.

Ignite-UX uses a separate directory for each client under `/var/opt/ignite/clients`. Each subdirectory is named based on the client's LAN address (LANIC, LLA, MAC address, etc). If you replace the client hardware, or even the LAN card that the old LAN address was based on, it will no longer access the same directory on the server.

The simplest solution is to obtain the new LAN address, which you can do from the Boot-ROM console command LanAddress (actual command may vary from system to system). Once you have the new address, then manually rename the directory. You may just remove the hostname symlink (it will be recreated automatically). Note that the LAN address must be in all upper-case, and begin with `0x`.

If you already booted the client from the server which caused it to create a new directory, you can just remove that directory before renaming the old directory. Be careful not to remove the original directory or else you will loose the recovery information. For example:

```
cd /var/opt/ignite/clients

mv 0x00108300041F 0x00108300042A

rm old_hostname
```

Volume group error

`Error: The minor number of the volume group exceeds the value IUX can support.`

See "Volume group error" on page 255.

Hot-swapping disks

Problem with hot swappable disks during recovery.

See "Hot-swapping disks" on page 255.

B Using a Boot-Helper System

A system running HP-UX 10.*x*, 11.0, or 11i can use the Ignite-UX server across a gateway if the target system is booted via the `bootsys` command. If the system is booted manually, it will need a helper system to help it boot across a gateway, and enabling the target system to perform this to the local boot-helper system:

```
boot lan.IP_address install
```

This chapter describes how to configure the boot-helper system.

To boot HP-UX across a gateway, you need a system on the local subnet to provide the target with a minimum core kernel. The helper system can run either HP-UX 10.*x*, 11.0 or 11i. The setup is much simpler if the helper system is running HP-UX 10.*x*, 11.0 or 11i.

6292
2

Setting Up the Boot-Helper

Follow these steps to setup and use a system on a remote subnet to allow a client to do a network boot and then contact a remote Ignite-UX server:

Setting up an HP-UX 10.*x*, 11.0 or 11i helper

Step 1. Install the Ignite-UX minimum core functionality onto the helper system:

```
swinstall -s /dev/rmt/0m Ignite-UX.MinimumRuntime
```

Step 2. On the helper, run the following command to point the INSTALLFS at the correct Ignite-UX server:

```
/opt/ignite/bin/instl_adm -t Ignite-UX_server_IP
```

Verify that INSTALLFS is referencing the correct Ignite-UX server, and gateway for your subnet:

```
/opt/ignite/bin/instl_adm -d
```

Step 3. Specify a temporary IP address for the helper. On the helper, in the /etc/opt/ignite/instl_boottab file, add the IP addresses that clients can use to boot. The remote subnet needs to have temporary IP addresses to use during an initial bootup. These are located in the /etc/opt/ignite/instl_boottab file, and were provided during the initial Ignite-UX server installation. But, the remote gateway systems cannot use these, so the boot-helper system must supply its own. Therefore create an /etc/opt/ignite/instl_boottab file on the boot-helper system containing lines of the following format. (See /etc/opt/ignite/instl_boottab on the Ignite-UX server for more details). For example:

```
15.1.53.180
15.1.53.181
15.1.53.182
```

Install Using a Boot-helper

Boot up the target machine to the `boot admin` menu, and boot from the helper system. For example:

```
boot lan.helper_IP_address install
```

If there's only one install server available on the subnet, then just enter:

```
boot lan install
```

At that point, the install should proceed, controlled from the server by default.

C Configuring for a DHCP Server

HP-UX 10.20 and Ignite-UX supports retrieving network information via the Dynamic Host Configuration Protocol (DHCP). This appendix describes setting up DHCP:

- Overview of DHCP Services.
- Setting Up a DHCP Server.
  - — Details of the DHCP Services.
  - — Enabling DHCP on a System Not Initially Configured with DHCP.
  - — DHCP Usage Examples.
  - — Using bootptab as an Alternative to DHCP.

Ignite allows for setting up DHCP for use during system installation. This appendix is for the user who wishes to use DHCP for ongoing IP address management, as well as for system installation.

6.288
2

Overview of DHCP Services

DHCP provides these features:

- Allows for dynamically allocating IP addresses and hostnames.
- Automatically supplies most of the networking defaults that are requested during a system installation or first time boot.
- Provides for on-going IP address maintenance via a concept of an "IP address lease." Having a lease on an IP address means that if the system "goes away" for a specified period of time without renewing the lease, then that IP address can be given to a different system that request a new IP address lease.
- Assists in re-establishing valid network parameters when a system has been moved from one DHCP-managed network to another.

DHCP works best under these conditions and restrictions:

- When a range of currently unused IP addresses can be allocated for use during new system bring-up.
- When the IP address-to-hostname mapping can be made ahead of time (before the system to use it is installed). And this mapping can be configured in the name services database before installing a system.
- When the IP address and hostname that get assigned to a system are not important. A system will keep the same IP address and hostname for as long as it renews the lease. However, the original assignment is arbitrary.
- When the person installing the systems does not desire to choose a hostname for the system, but rather accepts the one already registered for the IP address supplied by DHCP. This will ensure that the system will be recognized immediately by its hostname.

- When existing systems that did not use DHCP before will continue not to use it. Or, if they did, they would be willing to accept an arbitrary hostname and IP address. This is the same as with a new system. There currently is no tool available for pre-loading the DHCP database with existing IP addresses and identifying the systems they belong to. A tool to do this may be available in a future release.

An alternative to using DHCP is to create `/etc/bootptab` entries for each specific client on the network. This allows for specific IP address mappings and greater control. For more detail, please see “Using bootptab as an Alternative to DHCP” on page 275.

Setting Up a DHCP Server

Once you have decided that using DHCP will provide a benefit, you will need to follow the steps below to set up a DHCP server. *Note that only one DHCP server per network subnet is required.* On the server system:

- Allocate a set of currently unused IP addresses (preferably a contiguous block of addresses). For example:

  ```
  15.1.48.50 -> 15.1.48.80
  ```

- Pre-assign and register hostnames to the IP address allocated above. Using the `-h` option to the dhcptools command may be useful. For example, this command creates a `/tmp/dhcphosts` file that can be incorporated into your `/etc/hosts` or DNS/NIS database:

  ```
  dhcptools -h fip=15.1.48.50 no=30 sm=255.255.255.0 hn=de
  vlab##
  ```

- Designate a system to act as the DHCP server for your network. This should be a system that is "always" available to it's clients.

Use SAM to configure the DHCP services on this server:

Step 1. As root, enter: **sam**

(you may need to set your `DISPLAY` variable to use the graphical version)

Step 2. Double-click **Networking and Communications**

Step 3. Double-click **Bootable Devices**

Step 4. Double-click **DHCP Device Groups Booting From this Server**

You should now see a screen that lists any DHCP groups already defined (there may not be any if DHCP is not already configured).

Step 5. To add the new group of IP addresses which you allocated in Step 1, click **Action –> Add DHCP Group**

Step 6. Now fill in the information on this screen. Some information may require additional research if you are not familiar with the terms or with your network.

- **Group Name —** This can be any name that isn't already defined as a DHCP group. For example: `group1`

- **Subnet Address** — This is the portion of an IP address that is not masked off by the subnet mask (see below). If you don't want to figure this out, then just enter one of the IP addresses in the range you picked along with the correct subnet mask and SAM will take care of the calculation. For example: `15.1.48.50`

- **Subnet Mask** — This depends on the "class" of your network, and basically determines how an IP address is separated into a network number and a host specific number. Press **F1** in this field for more information. For example: `255.255.255.0`

- **Subnet Address Pool** — Press this button to select the range of IP addresses that you allocated in Step 1. A new screen will display where you can enter the Start and End address. If there are addresses within the range that you picked that you do not want allocated via DHCP, you can use the Reserved Addresses button to specify those (or ranges of them).

- **Allow Any Device Class** — The SAM default allows any type of DHCP device to use the group of IP address you are configuring. This may be undesirable if you use a different method (or a different DHCP server or group) for managing systems such as PCs running Windows98™ or NT™.

  If you want this range of addresses to be used only by HP-UX systems, then unselect this button, and in the text field provided enter: **`HewlettPackard.HP-UX`**

  When using Ignite-UX to set up DHCP, it will set a class specific to the server, and will set the `dhcp_class_id` string to match. For more detail, see the *instl_adm* manpage.

- **Automatic Allocation to Bootp Clients** — Leave this option disabled. Enabling it will cause problems for bootp devices such as printers and terminals which rely only on their preconfigured server to respond to their boot request.

- **Accept New Clients** — Leave this option enabled.

- **Address Lease Time** — The lease time should be set sufficiently long so that if a client system is temporarily out of service (`off`) for a time, its lease will not expire too soon.

  Infinite leases will never expire and disable the IP-address reclamation features of DHCP. For example: 2 weeks.

6.284

- **Boot file name** — You can leave this field blank.
- **Additional Params** — There are many parameters that can be specified in this screen for such things as the default routers, time server, DNS server, and NIS domain. You can specify as much or as little as you like in this area.
- **Callback Routines** — None are necessary.

Step 7. Once the parameters are all filled in, then press **OK** on the Add DHCP Group screen. SAM will then make the modifications to the `/etc/dhcptab` file.

Step 8. Click **Action** –> **Enable Boot Server** (if it is not already enabled).

New systems that are installed with HP-UX 10.20 or newer version or booted with a pre-installed HP-UX 10.20 or newer version should now contact this server to get an IP address lease and other network information provided by the server.

Details of the DHCP Services

- When cold-installing HP-UX 10.20 or newer:

  The installation tools will broadcast out on the network for any available DHCP servers. The first server to respond will be chosen to provide the default network information that the user is presented with.

  In the network parameters screen during a cold install, you see the question: `"Is this networking information only temporary?"` Responding `yes` or `no` answer to this question implies the following:

  — `no` (the default) means that if the IP address and hostname were leased from an DHCP server, then that lease will be retained after the install is done, so that the first boot of the system will attempt to renew the same lease.

  — `yes` implies that the IP address and hostname lease should be returned to the server after the installation is complete. In this case, the first system boot will try to get a new lease. This is most useful when the system is being installed on a network that is different from its final destination.

This answer to the question can also be set in the configuration file with the `instl_adm` command using the keyword: `is_net_info_temporary`

When automating system installations, the DHCP services allows systems to get networking information without mapping the Ignite-UX configuration files. For more information, see *instl_adm* (1M) and *instl_adm* (4).

- When a system boots for the first time (either after a cold install or the first boot of a pre-loaded (Instant Ignition) system):

  With HP-UX 10.20, the `auto_parms` and `set_parms` tools (they let you configure the system identity and basic configuration parameters) will invoke the `dhcpclient`, which will broadcast out to find a DHCP server. The server, in turn, provides a default set of networking parameters.

  With HP-UX 11.0, you are asked if DHCP should be enabled and used (by set_parms). The default is to *not* use DHCP.

  In both cold install and a first boot of a pre-loaded system, if the user chooses not to use the IP address given by the DHCP server, the tool will inform the DHCP server that it can release the lease on it and give it to someone else.

- At each system boot:

  If a client system was initially set up using an IP address that was leased by a DHCP server, that client will check to ensure that the lease is still valid at each boot. In addition, the system will start a daemon process (`dhcpclient -m`) that will maintain and renew that lease while the system is running.

  If a system cannot contact the DHCP server from which it originally got the IP address lease, it will try to contact other DHCP servers in order to determine if it has been moved to a different network. If this is the case, the system will write a message to the `auto_parms` log file (*/etc/auto_parms.log*) indicating that it has detected a move to a new subnet and that it is attempting to request a new lease. If the new lease request is successful, new networking configuration values supplied by the DHCP server will automatically be applied.

Enabling DHCP on a System Not Initially Configured with DHCP

If a system has been set up without using DHCP, but you would like to start using it, the following steps may be taken.

NOTE The system's hostname and IP address may change based on what the DHCP server assigns to it the first time it boots.

There are two methods for enabling DHCP on a system that is not currently using it:

Enable DHCP using SAM

Step 1. As root, run: `sam`

Step 2. Double-click **Networking and Communications**

Step 3. Double-click **Network Interface Cards**

Step 4. Highlight the card on which you wish to enable DHCP.

Step 5. Click **Actions** –> **Configure**

Step 6. Click **Enable DHCP**

TIP If **Enable DHCP** appears grayed-out, use the alternate method below.

Step 7. Click **OK** and exit SAM.

Your system will now begin using DHCP after the next reboot. Please note that all of the current networking parameters will be overridden with new values supplied by the DHCP server. *If for some reason the system cannot contact a DHCP server during the next reboot, it will continue to use its current networking parameters.*

If you suspect that your system had problem contacting the DHCP server, examine `/etc/auto_parms.log` to determine if the lease request was successful.

Alternate method

You can also enable DHCP over a particular network interface using a text editor such as vi or emacs to edit the /etc/rc.config.d/netconf file. In the header of this file, you will find some brief instructions regarding a variable named DHCP_ENABLE. This variable is tied by an index number to an individual network interface. For example:

```
INTERFACE_NAME[0]=lan0
IP_ADDRESS[0]=15.1.50.76
SUBNET_MASK[0]=255.255.248.0
BROADCAST_ADDRESS[0]=""
DHCP_ENABLE[0]=1
```

Here, the variables are instructing the system to use the lan0 interface when attempting to contact a DHCP server. Similarly, if the lease request is successful, the above IP_ADDRESS variable would be updated to reflect the new value supplied by the DHCP server.

If the DHCP_ENABLE variable was set to 0 or if the variable did not exist, no DHCP operations would be attempted over the corresponding network interface.

As noted in the first method of enabling DHCP, if the variable DHCP_ENABLE does not exist for a particular interface, SAM will display a grayed out DHCP enable button.

In this case, you will need to add the variable definition to a specific interface variable block. As an example, you would need to add DHCP_ENABLE[2]=1 to the following interface variable block in order to enable DHCP on the lan1 interface:

```
INTERFACE_NAME[2]=lan1
IP_ADDRESS[2]=15.1.50.89
SUBNET_MASK[2]=255.255.248.0
BROADCAST_ADDRESS[2]=""
```

The contents of /etc/rc.config.d/netconf for this definition block should now look like the following:

```
INTERFACE_NAME[2]=lan1
IP_ADDRESS[2]=15.1.50.89
SUBNET_MASK[2]=255.255.248.0
BROADCAST_ADDRESS[2]=""
DHCP_ENABLE[2]=1
```

Correspondingly, you could disable DHCP over a particular interface by setting the variable to 0.

Again, as in the first method, the system will only begin using DHCP after the next reboot.

DHCP Usage Examples

To enable a DHCP server to respond only to specific clients during an installation, use `instl_adm` to configure specific *dhcp_class_id*s.

Your situation might fall into one of these categories:

- The network has a DHCP server that manages the whole network, and the clients doing installations will be using the addresses from this server permanently. In this case, do nothing since this line is entered in `INSTALLFS` file by default:

  ```
  is_network_info_temporary=false
  ```

- The network has a DHCP server, but the user would like to manage a small group of temporary IP addresses, just for use in doing installations, and the clients will get reassigned new addresses when deployed.

Step 1. Set up DHCP on Ignite-UX server.

Step 2. Use a unique *dhcp_class_id* in both the `dhcptab` and the 8KB config file. This *dhpc_class_id* could include the server's hostname. In this case, enter the following in `INSTALLFS` using `instl_adm`:

```
is_network_info_temporary=true
```

Step 3. Enter your class ID as the following in the dhcptab and `INSTALLFS`:

dhcp_class_id

If you have a non-HP server that does not recognize `dhcp_class_id`, specify the server using the `dhcp_server` keyword instead.

- The user would like to setup the Ignite-UX server as a "departmental" DHCP server, in which case the IP address leases are permanent, but they will be isolated to the department's DHCP server.

Step 1. Set up DHCP on the Ignite-UX server.

Step 2. Enter this line:

```
is_network_info_temporary=false
```

Step 3. *And* enter your class ID as the following in the dhcptab and INSTALLFS:

dhcp_class_id

(Or use the dhcp_server keyword as explained in the previous Step 3 above.)

Use a unique *dhcp_class_id* in both the dhcptab and the INSTALLFS file. This *dhcp_class_id* could have the server's hostname in it.

- You want to start using DHCP with this server managing the whole network. Refer to the preceding sections, /usr/sbin/sam, and the *sam*(1M) manpage for this procedure.

For more information, see the *setup_server* (1M) and *bootpd* (1M) manpages.

Using bootptab as an Alternative to DHCP

If you want to have more control over the allocation of IP addresses and their mappings to your clients, you can configure entries in /etc/bootptab for each client. Because BOOTP protocol is a subset of DHCP protocol, the client's request for a DHCP server will be satisfied with the BOOTP response.

If you also specify a boot-file (bf) of /opt/ignite/boot/boot_lif in the bootptab entries, then you do not need any additional entries in /etc/opt/ignite/inst_boottab. In this case, you would then boot the clients using boot lan instead of boot lan install. Only clients known in /etc/bootptab would be able to boot if you do not use instl_boottab.

A minimal example /etc/bootptab entry is shown below (use your own hostname, IP address, hardware address, and subnet mask). Other networking information may also be specified here or via instl_adm. Specify the Ignite-UX server's IP address with the instl_adm -t option.

```
sysname:\
  hn:\
  vm=rfc1048:\
  ht=ether:\
  ha=080009352575:\
  ip=15.1.51.82:\
  sm=255.255.248.0:\
  bf=/opt/ignite/boot/boot_lif
```

Background Information on DHCP Design

The DHCP protocol is implemented as extensions to the BOOTP protocol, and in fact the HP-UX DHCP server daemon and the BOOTP daemon are the same: `bootpd`. This daemon reads two configuration files: `/etc/bootptab` and `/etc/dhcptab`.

The mapping of systems to IP addresses and lease time information is kept in the DHCP database file `/etc/dhcpdb`. Some amount of management of this database is provided by the `dhcptools` command.

On the client side, a command called `/usr/lbin/dhcpclient` is used to contact the server to get an IP address lease. This command has the ability to broadcast out onto the network prior to the network interface being enabled.

The `dhcpclient` also serves as a daemon process that sleeps until the time that it needs to renew the IP address lease, at which time it will re-contact the server where it got the original lease in order to extend it.

The `dhcpclient` command is not intended to be run by users directly, and is called by other tools during system bootup and installation.

For More Information

See the *auto_parms* (1M)and *dhcpdb2conf* (1M) manpages for more information regarding the networking parameters which DHCP can supply.

More general information on DHCP can be found in the following locations:

- Manpages:

  bootpd (1M)
  dhcptools (1M)
  auto_parms (1M)
  dhcpdb2conf (1M)

- Web:

  `www.dhcp.org`

Index

Index

Apêndice EB

» hp home | » products & services | » support & drivers | » solutions | » how to b

» contact hp

search: » more o|

● software depot ○ all of hp US

printable ve

mirrordisk/ux license for servers

» software depot

» electronic (re)download
» how to buy support
» hp-ux OE product information
» hp-ux 11i promotions

product details & specifications

overview

MirrorDisk/UX License for Servers
Introduction

MirrorDisk/UX software prevents data loss due to disk failures by maintaining up to thre(data on separate disks. Applications can continue to access data even after a single dis addition, you can perform on-line backups to avoid user and application disruption.

To prevent the failure of a single I/O interface from causing a system failure, HP recomn mirrored disks be connected to separate interface cards.

Features and Benefits

- No single point of failure - separate controllers/power supplies
- Up to 3-way disk mirroring
- On-line backup while maintaining mirroring
- Application transparency
- Dynamic mirror configuration
- Selective mirror of data
- Fast data synchronization
- Menu-driven administration tools

Because high availability solutions require full-time access to data, HP has developed M to provide mirroring capability within the HP-UNIX® Operating System (HP-UX) environ

MirrorDisk/UX, the mirroring component of Logical Volume Manager (LVM) from the Op Foundation (OSF™), prevents data loss by maintaining up to three copies of data on se This enables data to remain intact after a single disk or interface card failure.

MirrorDisk/UX can mirror a disk partition, including the root and swap partitions. It suppc of raw disk access as well as file system access. MirrorDisk/UX can increase input/outp performance depending upon the mix of disk reads and writes.

Because MirrorDisk/UX works with the HP-UX kernel to manage the mirrored disks, it is to the applications, which require no modification.

MirrorDisk/UX allows customers to perform a backup by taking one disk of a mirrored pa while the other disk continues to service applications. As the backup is being performed occurring to the online disk are maintained in table memory. Upon completion of the bac procedure, a faxt update is done to synchronize the disks while application continuity is To prevent the possibility of data loss caused by a failure during a backup, three-way mi provides a fully redundant mirrored pair while the third copy is being backed up.

Date: 6/21/99

additional product information

product #:	B2491BA
version:	-
software specification:	Server, HP-UX11.00 Server, HP-UX11.11
price:	$1017.00 Per Processor License

» support

buy from

privacy statement

using this site means you accept its terms

Apêndice EC

hp rack-optimized
rp5430 and rp5470
servers
entry-level UNIX® servers

hp servers
product brief

hp rack-optimized servers can help you be always on, always there, always connected

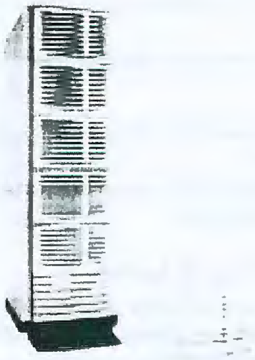
hp servers rp5430 and rp5470: smart, simple, stress-free

In today's economy, whether you're managing your own IT infrastructure or hosting someone else's, you have to operate with a faster time-to-solution, within budgetary constraints, and with the highest standards for customer service and operational efficiency.

To create and run an infrastructure for an always-on business, you need a computing platform that will support the way you—and your customers—do business. The HP Servers rp5430 and rp5470 give your business the fastest—and most reliable—means of succeeding in this new business environment.

The HP Servers rp5430 and rp5470 deliver the proven performance, scalability, and high-availability capabilities of UNIX—without high maintenance requirements and costs. And they give you plenty of room to grow. You can start at a low-price entry point and scale up to the leading 4-way UNIX performance—in the same rack-optimized form factor, without penalty. And with its industry-leading solution partners, HP has developed business solutions surrounding these servers that are tested, easy to deploy, and easy to manage.

With HP Servers rp5430 and rp5470, owning and operating a UNIX server is smart, simple, and stress-free.



hp servers rp5430 and rp5470

smart

HP Servers rp5430 and rp5470 offer leading entry-level server performance, dynamic scalability, and unmatched investment protection—all in a rack-optimized package—making them the smart choice for the most demanding applications.

leading performance—scalable functionality

- industry-leading OLTP performance
- massive bandwidth for I/O-intensive applications
- 7U-height and packed with CPUs, memory, and I/O, plus the ability to scale subsystems without compromise
- rack-optimized to make the best use of valuable data-center floorspace

unparalleled investment protection

- industry's only in-box upgrade from 2-way to 4-way UNIX computing
- built-in growth path to the HP Server rx5670, featuring Intel® Itanium® 2 processors

proven solutions for business-critical computing

simple

hp makes IT easy

With HP Servers rp5430 and rp5470, HP offers a unique combination of solutions designed to help you get started quickly and manage your IT environment effectively.

hp-ux: robust, proven enterprise operating environment for mission-critical applications

- industry-leading performance, scalability, availability, manageability, and security
- pre-packaged, integrated, and production-ready operating environments
- industry-leading Windows® and Linux interoperability
- centralized software updates that are timely, simple, and efficient
- powerful alliances with industry-leading software vendors and systems integrators to deliver robust solutions from e-commerce to enterprise resource planning (ERP) and beyond

leading-edge management capabilities with hp-ux virtual partitions and hp-ux workload manager

- system resource optimization enabling multiple workloads to run simultaneously on the same server, each with their own instance of HP-UX
- improved security and server availabilty through complete software and operating system isolation
- HP-UX Virtual Partitions integrate with HP-UX Workload Manager for the most efficient resource distribution across partitions, in a single server
- base offering complementary with HP-UX 11i for your HP Server rp5470

integrated management capabilities

- HP Servicecontrol Manager and integrated HP Secure Web Console capability for full remote management, including centralized configuration of multiple servers

the right server for today's applications

ERP (supply-chain management)
High availability, leading-edge manageability, and scalable performance support demanding end-to-end enterprise applications.

broadband
The combination of leading performance, I/O throughput, and capacity and high availability with end-to-end solutions delivers more powerful, reliable broadband services.

Internet infrastructure
Highly scalable, reliable, and manageable Web server, caching server, load balancing, e-commerce server, firewalls, or mail server.

e-commerce
Leading performance and I/O bandwidth, in-box scalability, rack-optimized form factor (five per standard 2-meter rack), high availability, and Internet management features.

technical computing
Leading performance and throughput, N+1 redundant components, extensive memory capabilities, and clustering solutions to meet the demands of computation, NFS file serving and product data management, and Web hosting.

flexible financing

- operating leases with a variety of attractive terms
- the Tech Refresh program for cost-effective upgrades to stay on the leading edge of new technology
- bundled Solution Finance program to consolidate and simplify financing arrangements

instant capacity on demand for your hp server rp5470

iCOD

- instant activation of incremental CPU power when you need it
- pay only for the processing power you use

temporary capacity for iCOD

- temporary activation of incremental CPU power for a limited period
- ideal for short-term, predictable processing demands

stress-free

make your business your focus

The HP Servers rp5430 and rp5470 handle the demands of users efficiently and reliably—so you can concentrate on running your business, not managing your IT resources.

high availability for continuous operations

- a rich set of in-box high-availability features
- affordable high-availability clustering solutions based on industry-leading HP MC/Serviceguard
- self-healing capabilities, a first for entry-level servers—proactively avoid faults to improve uptime
- a critical building block for your always-on e-business needs

total solution support

- options ranging from Web-based services to the industry's only 6-hour call-to-repair commitment
- "one-stop" solution support delivered with partners such as Cisco, Oracle®, SAP, i2, Inktomi, and many more

best UNIX server family—top to bottom

The low-cost entry point to the two-way HP Server rp5430 through the more scalable HP Server rp5470 are part of the powerful HP UNIX server line—servers that set the standards for business-critical computing and total cost of ownership. Simple in-chassis upgrades let you move up the line as your business grows. HP UNIX servers provide the hardware foundation for an Internet infrastructure that is always on. Combining leading technology with proactive and reactive services, HP offers complete, end-to-end solutions that include hardware, software, applications, services, support, consulting, and an extensive portfolio of experienced partners, so you can get to market quickly with a single source of expertise. The HP UNIX server family is robust from the top to bottom—from the high-end HP Superdome; through the HP Servers rp8400 and rp7410, the midrange performance and price/performance leaders; and to the scalable entry-level HP Servers rp5430 and rp5470. Rounding out the family are the hyper-dense HP rp2400 series servers for Internet applications and branch offices.

hp servers rp5430 and rp5470 features and benefits at-a-glance

features	benefits
smart	
1–4 (rp5470) or 1–2 (rp5430) 875MHz PA-8700+ CPUs with 2.25 MB on-chip cache per CPU or 750MHz PA-8700 CPUs with 2.25 MB on-chip cache per CPU	Superior performance over comparable systems, with plenty of headroom for growth
Up to 16 GB (rp5470) or up to 8 GB (rp5430) SDRAM memory with advanced ECC protection	Fast and reliable processing power for frequently accessed data
Up to 10 (rp5470) or 6 (rp5430) PCI I/O slots with 3.2 GB/s (rp5470) or 2.3 GB/s (rp5430) I/O bandwidth	Easily handles I/O-intensive applications and allows the system to scale I/O, CPUs, and memory without compromise
Core I/O, including 10/100Base-T LAN with auto speed-sensing, a second 10/100Base-T support LAN, Ultra2 LVD SCSI, and RS-232	Provides easy, ready-to-go networking capabilities
Up to 4 internal 36 GB, 73 GB, or 146 GB Ultra320 SCSI hot-plug high-uptime disks	Store critical data with massive internal capacity
1 internal DVD or DAT drive	Protects critical data
7U chassis with up to 5 servers per standard 2-meter rack; also available in standalone (pedestal) configuration	Optimizes use of floor space and delivers high-performance density in a racked configuration
Easy in-box upgrades from the rp5430 to the rp5470	Architectural scalability ensures these servers can grow with the business, maximizing flexibility and investment protection
Support of Intel Itanium Processor Family as well as PA-RISC processors	Provides investment protection through dual growth paths
simple	
Built-in unlimited user license for proven 64-bit HP-UX 11i and 11.0	Proven, enterprise UNIX operating system for mission-critical applications
HP Virtual Partitioning for the rp5470	Maximizes usage of computing resources
Integrated HP Secure Web Console and Servicecontrol Manager for full local, Web, and remote control of servers	Provide complete single-system and multisystem administration capabilities, including a range of security features, from any browser-based PC
Flexible financing programs	Make initial ownership and modular growth easy and affordable
Instant capacity on demand (iCOD); temporary capacity for iCOD	Immediate access to CPU power when you need it, either permanently or temporarily
HP global deployment and partner integration services	Offer guaranteed error-free solution deployment to reduce implementation time and cost
HP On-site Solution consolidated manufacturing, streamlined product assembly and testing, and state-of-the-art integration	Ensure superior quality and faster delivery
stress-free	
Error-correcting cache, parity checking on all buses, memory scrubbing and page de-allocation, dynamic processor resilience, and de-allocation of application processes Dual Ultra 2 SCSI buses and controllers for mirrored storage Hot-swap, redundant power supplies and fans; redundant, hot-plug PCI; Ultra2 SCSI hot-plug disks	Built-in high-availability features deliver superior levels of • error correction, • error containment, • data protection, and • serviceability to help maximize uptime for business-critical workgroups and applications
Integrated Event Monitoring Service (EMS) Built-in fault management system with separate support processor and bus Integrated with HP MC/Serviceguard, HP Toptools for Servers, and enterprise management software such as HP OpenView and CA Unicenter	Provides superior system uptime through constant, proactive fault avoidance, detection, and notification; monitors power, cooling system hardware, processors, memory, HP-UX resources, and external storage
Pre-tested and pre-integrated workgroup clustering solutions based on HP MC/Serviceguard	Deliver complete, ready-to-go solutions for clustered high availability that eliminate all single points of failure, at an affordable price
3-year on-site service warranty and HP services and support options ranging from Web-based support to mission-critical, 6-hour Call-to-Repair commitment; includes full solution support for hardware and software	Reduce risk through worldwide support for business-critical computing; provide "one-stop shopping" for support through partnerships with Cisco, Oracle, SAP, BroadVision, Inktomi, and others

stay ahead of the curve

configuration options	hp server rp5430	hp server rp5470
processor	875MHz PA-8700+ or 750MHz PA-8700	875MHz PA-8700+ or 750MHz PA-8700
SMP configuration	1 to 2 CPUs	1 to 4 CPUs
supported OS versions	HP-UX 11i PA-8700+ HP-UX 11.0, 11i PA-8700	HP-UX 11i PA-8700+ HP-UX 11.0, 11i PA-8700
minimum/maximum memory	512 MB/8 GB	512 MB/16 GB
on-chip cache (data/instr)	1.5 MB/750 KB	1.5 MB/750 KB
total I/O slots	6	10
internal removable media bays	1	1
maximum internal disk capacity	584 GB (4 disk bays)	584 GB (4 disk bays)
standard I/O features	Ultra2 SCSI, 100Base-T LAN, 3 RS-232 ports, 100Base-T support LAN, and Web-based console	
supported I/O connectivity	Ultra2 SCSI RAID, Ultra2 SCSI LVD (single- and dual-port), FWD SCSI (single- and dual-port), Fibre Channel, Gigabit Ethernet, 100Base-TX (single- and quad-port), 100Base-FX, ATM 155 Mb/s (MMF, UTP-5), ATM 622 Mb/s (MMF), FDDI dual-attach LAN, Token Ring 100 Mb/s; X.25/FR/SDLC (dual-port), multiplexer (8- and 16-port)	

environmental specifications	
electromagnetic interference	Complies with FCC Rules and Regulations, part 15, as a Class A digital device; Manufacturer's Declaration to EN 55022 Level A; VCCI Registered, Class I; Korea RLL
AC input power	100-240V 50/60Hz
maximum current requirements	13.8A at 110V
maximum power dissipation	1283 watts
physical dimensions	Depth: 774 mm (30.5 in) Width: 482 mm (19.0 in) Height: 368 mm (14.5 in)/7 EIA units Weight: 68 kg (150 lb)
operating temperature	+5° to 35°C (41° to 95°F)
nonoperating temperature	–40° to 65°C (–40° to 149°F)
maximum rate of temperature change	20°C/hour
operating relative humidity	15% to 80%, noncondensing, max. wet bulb @ 26°C
nonoperating relative humidity	5% to 90%, noncondensing
operating altitude	To 3.0 km (10,000 ft) above sea level
nonoperating altitude	To 4.5 km (15,000 ft) above sea level
compliance model number	RSVL - 0105-A

for more information

Contact any of our worldwide sales offices or HP Channel Partners (in the U.S. call 1-800-637-7740) or visit the HP servers Web site at **www.hp.com/go/servers** or **www.hp.com/go/rp5430** or **www.hp.com/go/rp5470**

HP product information and technical documentation are available online. In addition, configuration tools and pricing information allow registered users to place orders online.

hp®

invent

Apêndice ED

hp serviceguard extension for RAC

proven, flexible high-availability solution

the challenge

To maintain and manage a highly available mission-critical parallel database environment

the solution

HP Serviceguard Extension for RAC

business benefits

- data protection
- application availability
- ease of management
- flexible and easy deployment of applications
- expert consulting and support services

To best meet data center requirements for availability, flexibility, and scalability, HP offers a robust architecture that combines multiple computers into entities called "clusters." The systems—or nodes—of a cluster are connected in a loosely couplec manner, each maintaining its own separate processor(s), memory, and operating system. Special communications protocols and system processors bind these nodes togethei and allow them to cooperate to provide outstanding levels of availability and flexibility for supporting mission-critica applications.

Clusters maintain strict compliance to the principles of open systems. There are no propriety APIs that force vendor lock-in and require substantial development investment. Most applications will run in a cluster without any modification at all. And only standards-based hardware components such as SCSI or Fibre Channel storage devices and FDDI Ethernet LANs are used to create a cluster.

Clusters provide a cost-effective, flexible architecture for meeting the demanding requirements of the commercial UNIX® market.

Building on the superior capabilities of HP Serviceguard, HP Serviceguard Extension for RAC (formerly called Serviceguard OPS Edition) allows a group of HP 9000 servers to be configured as a highly available cluster that supports Oracle9*i* Real Application Cluster (RAC) on both HP-UX PA-RISC and Intel® Itanium™ Processor Family platforms. These two products are tightly integrated to provide the best aspects of HP enterprise clusters and Oracle® relational database servers: high availability, data integrity, flexibility, scalability, and reduced database administration costs.

scaling beyond one system

Oracle9*i* RAC-enhancing scalability

With the introduction of Oracle9*i* Real Application Cluster (RAC), the unique architecture of a Serviceguard Extension for RAC cluster enables the full aggregate processing power of up to 16 nodes to access the database, increasing overall throughput for certain kinds of applications. Examples of applications that can benefit from the performance gains and scalability of this cluster include query-intense applications such as decision support, applications that generate random reads and writes to very large databases, and applications that access separate partitions of the database.

enhancing performance

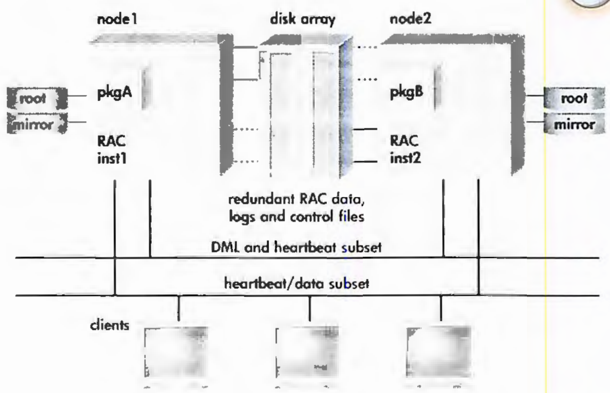
The new HP Hyper-messaging Protocol with Oracle9*i* RAC provides high-bandwidth, low-latency server-to-server communication that promises to deliver superior interconnect performance.

serviceguard extension for RAC

Serviceguard Extension for RAC provides all of the functionality needed to support the Oracle9*i* RAC environment on HP 9000 servers. The major components of Serviceguard Extension for RAC are listed here.

- **cluster manager:** establishes and monitors the cluster members and monitors various components within each node
- **cluster membership:** informs RAC about system failures to facilitate fast database recovery
- **package manager:** monitors and controls packages containing highly available applications
- **network manager:** detects and recovers from card and cable failures
- **shared logical volume manager** (ships with HP-UX): provides the basic functionality to share physical disks and buses between the nodes

Serviceguard Extension for RAC also provides further enhancements to the environment needed to support mission-critical applications. Special functionality is included to significantly enhance the availability of each node within the cluster and to provide extra protection for database integrity. Since high availability is a primary design goal, this cluster has been created with no single point of failure. The data disks are mirrored via a disk array, and multiple LANs are used.



key features and benefits

data protection

- multiple cluster arbitration mechanisms prevent failed nodes from jeopardizing the integrity of application data

availability

- local area network (LAN) monitoring ensures quick, transparent recovery to maximize database availability
- quick automatic detection and recovery time maximizes application availability and minimizes operator error
- the ability to survive multiple node failures provides a unique level of protection
- fast failback shortens startup time for applications in the primary active node
- rolling upgrades ensure application availability during hardware and software maintenance
- integration with HP Workload Manager ensures service-level objectives (SLOs) are maintained during planned and unplanned downtime
- tight integration with Oracle's specialized RAC HA Extension configuration offers quicker detection and failover
- the Enterprise Cluster Master toolkit provides quick and easy deployment of applications
- extended-distance clustering (up to 10 km) provides disaster-tolerant protection

flexibility

- multiple cluster configurations—active-active, active-standby, and rotating standby—offer flexibility

manageability

- an intuitive graphical user interface, Serviceguard Manager, reduces the total cost of managing multiple clusters from a single console
- support for virtual and hard partitioning addresses the increasing demand for systems consolidation

ROI

- integration with HP Pay per Use offers a cost-effective disaster-tolerant solution that is unique to HP

one call, one voice

hp and Oracle: joint facilities

To provide consulting and support expertise for customers working with enterprise clusters, HP and Oracle maintain joint facilities staffed with technical experts. These facilities are available for developing proofs-of-concept for new projects, executing benchmarks, and performing sizing activities for enterprise clusters.

support services

HP understands that ensuring a highly available mission-critical environment means more than just having the right technology—it is just as critical to have the right IT processes and support services in place. That's why HP has created a comprehensive portfolio of services, ranging from consulting, education and training, and disaster planning and recovery services to mission-critical support for HP hardware and software products—including Serviceguard Extension for RAC.

- **personalized systems support (PSS):** a comprehensive support solution. PSS combines proactive account services with industry-leading technical assistance to help you improve operational effectiveness and successfully manage and implement change within your IT environment.
- **business continuity support (BCS):** emphasizes downtime prevention through continuous improvement of your IT infrastructure, the best mission-critical processes, and constant vigilance. BCS starts with an extensive assessment to identify and analyze areas that put availability and service-level requirements at risk, and then it presents recommendations to minimize these risks.
- **critical systems support (CSS):** provides technical expertise through an integrated combination of proactive services and fast problem resolution to meet the demands of your computing environment. Also available through CSS is a portfolio of technical services designed to minimize system problems and downtime and to help you make more effective use of technology. Areas of interest include high-availability technologies, performance analysis, change planning, security review, and system administration.

value-added hp services

Because continued proactive management of your cluster is critical to ensuring high availability HP has introduced an additional technical service to help increase cluster availability and stability.

- **hp cluster consistency service (H8395AT)**—delivers a diagnostic tool for spotting potential disruptions to critical applications by identifying cluster configuration problems before they occur.

benefits of hp services

By taking advantage of HP services, you will realize major benefits:

- reduced implementation time with expertise, partnership, and hands-on assistance from your assigned high-availability–certified HP team
- decreased IT crisis risk and exposure through robust proactive services
- increased availability due to improved environment stability and rapid problem resolution through established and proven processes
- maximized end-user productivity thanks to optimized processes and system performance
- comprehensive planning support using proven HP methodology

more information

For more information, please visit our Web sites at
www.hp.com/hps
www.hp.com/go/financialservices

www.hp.com/go/ha

hp®
invent

Intel and Itanium are trademarks or registered trademarks of Intel Corporation in the U.S. and in other countries and are used under license. Oracle is a registered U.S. trademark of Oracle Corporation, Redwood City, California. UNIX is a registered trademark of The Open Group.

Technical information contained in this document is subject to change without notice.

12/02
5981-4712EN

Apêndice EE

hp server rp5400 series entry-level UNIX servers

August 2002

a technical white paper from Hewlett-Packard

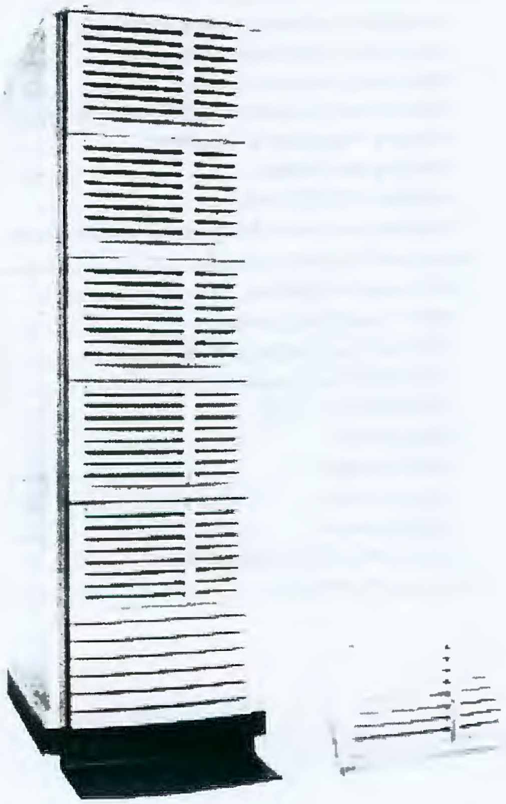


table of contents

introduction to the hp server rp5400 series

In today's economy, whether you're managing your own IT infrastructure or hosting someone else's, you have to operate with a faster time-to-solution, within budgetary constraints, and with the highest standards for customer service and operational efficiency.

The HP Server rp5400 series gives you the fastest and most reliable means to succeed in this new business environment. The rp5400 series consists of two products that deliver the proven performance, scalability, and high-availability capabilities of UNIX®—without high maintenance requirements and costs. And they give you plenty of room to grow. You can start with a low-price entry point and scale up to the leading 4-way UNIX performance—in the same form factor.

The rp5400 series is made up of two different servers, each with a unique ability to match your computing needs. The rp5430 is a 2-way system with time-proven, cost-effective PA-RISC technology. It offers the latest PA-8700+ processors and the same high-performance core electronics found in more expandable HP servers. The rp5470 is the high-performance flagship of the lineup. It supports up to 4-way PA-8700+ processing power and industry-leading bandwidth.

Both members of the rp5400 series use the same rack-optimized 7U package. This allows seamless scalability with simple in-box upgrades between servers in the series. Additionally, the rp5400 series was designed for board-swap upgrades to the Itanium 2-based HP Server rx5670. Together, the rp5400 series offers the industry's best 1- to 4-way lineup with unparalleled investment protection.

figure 1.1 a front view of the rp5400 series

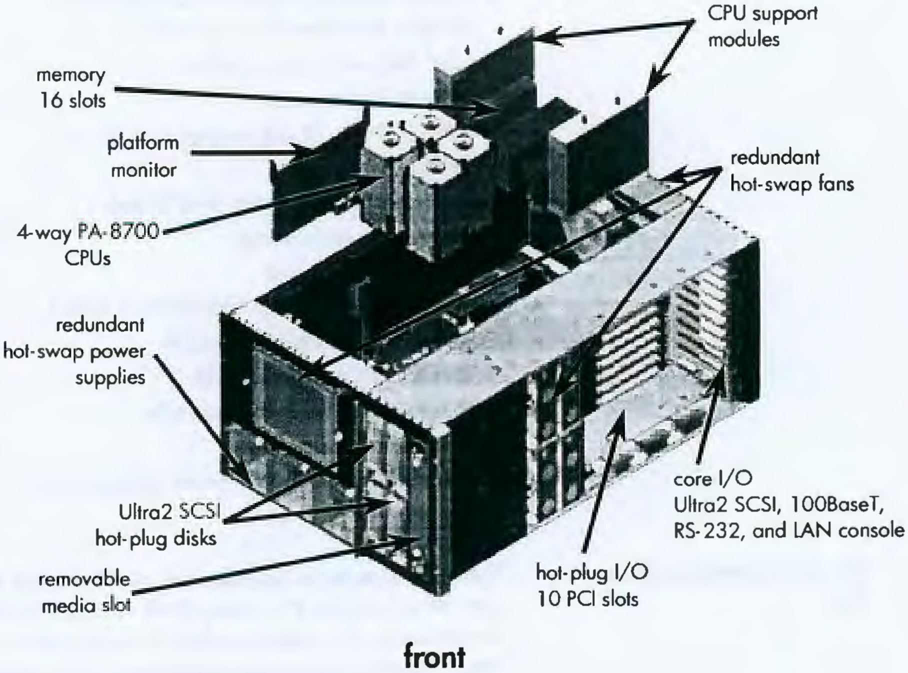

CPU support modules
memory 16 slots
platform monitor
redundant hot-swap fans
4-way PA-8700 CPUs
redundant hot-swap power supplies
core I/O Ultra2 SCSI, 100BaseT, RS-232, and LAN console
Ultra2 SCSI hot-plug disks
hot-plug I/O 10 PCI slots
removable media slot
front

Figure 1.1 reveals the location of major components, as well as the mechanical and architectural features of the rp5400 series. The server is partitioned into two main electrical assemblies—the system board and the I/O backplane—and into three main volumes—processor and memory, I/O and disk, and power.

Looking at the front face, three hot-swap power supply bays are located in the lower left corner. To the right, a peripheral bay provides space for four hot-plug disks and one removable media device (either DVD-ROM or DDS-3). Directly above the power supply bays is the first of eight hot-swap cooling fans.

The right side of the system houses the I/O card bay. There are ten PCI I/O slots available. Two pairs of fans located here provide cooling for the I/O bay as well as the peripheral bay.

The opening at the top provides access to the system board, which supports the four CPUs, sixteen dual inline memory module (DIMM) slots, two processor support modules, and the platform monitor board. The core I/O is located at the rear of the system.

rp5430 features at-a-glance

- 1 to 2 PA-8700+ or PA-8700 CPUs
- 875MHz and 750MHz CPUs
- high-performance "stretch" core electronics complex (leveraged from rp7400)
- Intel® Itanium® 2 upgradable
- up to 8GB of memory
- 6 PCI I/O slots (5 are hot-plug 66MHz × 64-bit)
- 6 independent PCI buses for I/O slots
- N+1 power and cooling
- 4 hot-plug disk drives
- removable media bay: DVD-ROM or DDS-3
- 4.3GB/s system bus bandwidth
- 2.1GB/s I/O bus bandwidth
- 4.3GB/s memory bus bandwidth
- 64-bit HP-UX 11.0 & 11i
- high-density 7-EIA-unit, 19-inch rackmount or pedestal package

rp5470 features at-a-glance

- 1 to 4 PA-8700+ or PA-8700 CPUs
- 875MHz and 750MHz CPUs
- high-performance "stretch" core electronics complex (leveraged from rp7400)
- Intel Itanium 2 upgradable
- up to 16GB of memory
- 10 PCI I/O slots (8 hot-plug, 2 non-hot-plug; all are 66MHz × 64-bit)
- 9 independent PCI buses for I/O slots
- N+1 power and cooling
- 4 hot-plug disk drives
- removable media bay: DVD-ROM or DDS-3
- 4.3GB/s system bus bandwidth
- 3.2GB/s I/O bus bandwidth
- 4.3GB/s memory bus bandwidth
- 64-bit HP-UX 11.0 & 11i
- high-density 7-EIA-unit, 19-inch rackmount or pedestal package

the hp server product line

The rp5400 series is the entry-level cornerstone of the business-critical proven HP server product line. HP servers are #1 among UNIX servers for reliability, scalability, availability, and price/performance. This robust product line addresses the major computing challenges customers face today in online transaction processing (OLTP), electronic commerce (ECOM), Internet/intranet serving (Web), enterprise resource planning (ERP), supply chain management (SCM), and technical applications.

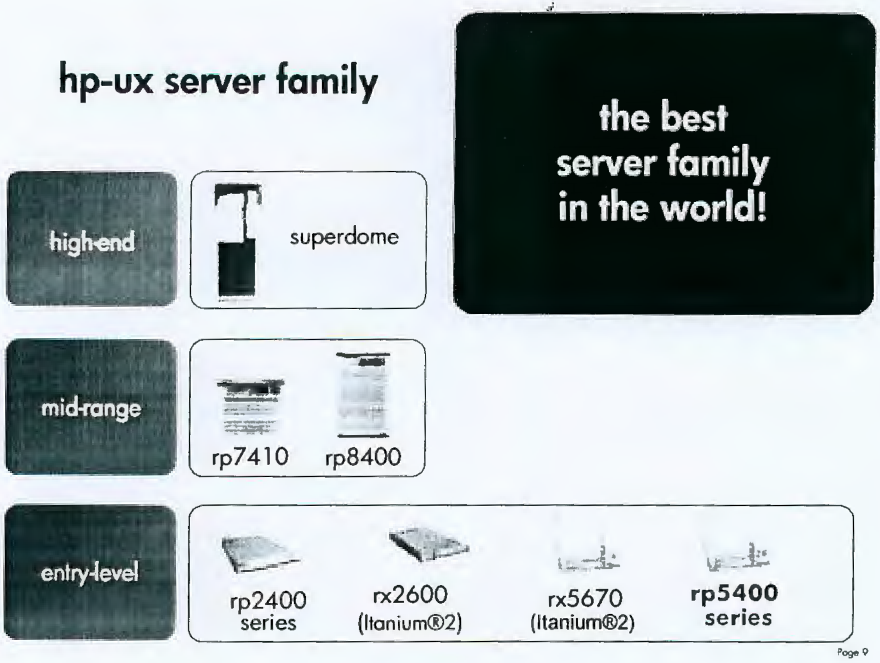
At the low end, affordable rp2400 and rp5400 series servers effortlessly handle Internet workloads and enterprise-size applications. Both platforms also add leadership price/performance and include bundled Internet software solutions.

In the midrange, the rp8400 and rp7410 deliver the high-performance, compact Internet-era UNIX server platform that today's IS executives are demanding. With up to 16 PA-8700+ processors, the HP server midrange lineup provides the robust performance and scalability needed for the most demanding workloads.

With exceptional OLTP performance, availability, scalability, and manageability, HP Superdome has become the pacesetter for high-end computing. Superdome, coupled with HP's always-on infrastructure strategy, provides UNIX application performance and Internet-critical high availability to help you meet the rigorous demands of e-services and systems consolidation, as well as large-scale, highly complex technical modeling and simulations.

All of HP's UNIX servers provide excellent investment protection with a smooth transition path to future PA-RISC and/or Itanium-based architectures. So whether your business requires cutting-edge e-services, systems consolidation, or a host of other solutions, our power-packed servers are business-critical proven and ready to meet the challenge—today and tomorrow.

figure 1.2 the industry's strongest UNIX lineup—top to bottom



binary compatibility

The rp5400 series supports the 64-bit HP-UX 11 operating system. With HP-UX 11, HP maintains its longstanding tradition of providing the industry's best record of investment protection. HP-UX provides forward binary compatibility, in which a fully bound application developed on an earlier version of HP-UX is ensured to run smoothly on HP-UX 11. Thus, current 32- and 64-bit applications can run without requiring recompilation.

Intel Itanium Processor Family ready

The rp5400 series was designed for several generations of PA-RISC and is upgradable to the Itanium 2-based HP Server rx5670. HP offers a board-swap upgrade to move any rp5400 series product or any legacy HP 9000 L-Class product to the Intel Itanium Processor Family.

The Intel Itanium Processor Family is based on Explicitly Parallel Instruction Computing (EPIC), a new architecture technology invented by HP Labs. The EPIC architecture breaks through the sequential nature of today's RISC and CISC processor architectures by allowing the software to communicate explicitly to the processor when operations can be done in parallel. EPIC serves as the enabler for future high-performance chips by providing explicit parallelism, massive resources, and inherent scalability not available with conventional RISC architectures. Increased performance is realized by reducing the number of branches and branch mispredicts and by reducing the effects of memory-to-processor latency.

Intel Itanium Processor Family transition

For the vast majority, the transition to the Intel Itanium Processor Family will be simple and seamless. For customers who require additional assistance, HP provides transition services around the world to help make this upgrade as smooth as possible. HP can provide assistance every step of the way, from assessment and design to verification and deployment. Consult the Intel Itanium processor section of HP's Web page for further information.

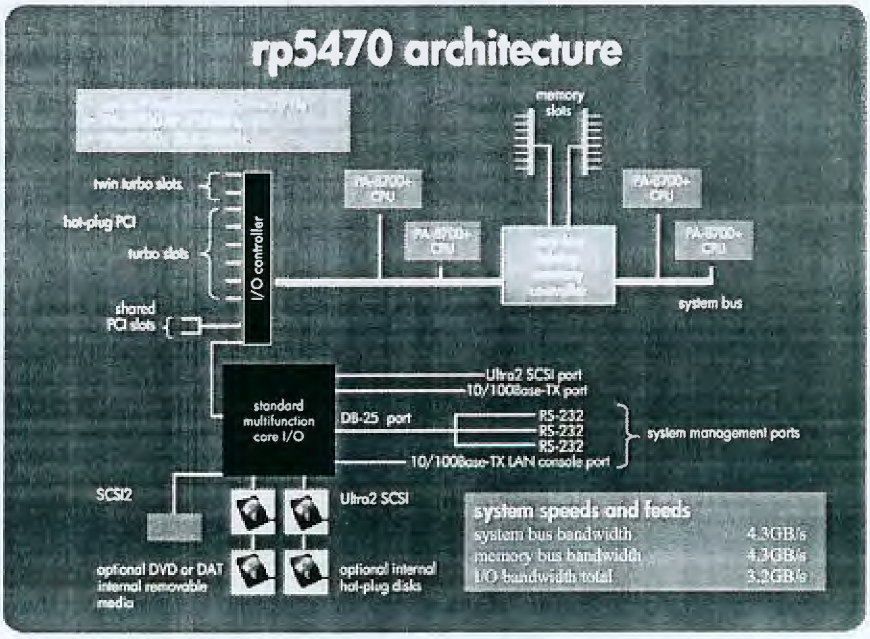
architecture

Figure 2.1 shows the relationship of the rp5470 main blocks with the buses that connect them. The rp5470 uses the "stretch" high-performance core electronics complex (CEC), which is also used in the midrange rp7400 server. This CEC, specifically designed for demanding Internet workloads, brings unprecedented levels of bandwidth and performance to the 4-way entry-level market.

Two front-side buses, both running at 133MHz, provide 4.3GB/s of bandwidth to four PA-8700+ or PA-8700 processors. The low-latency memory controller provides 4.3GB/s of memory bandwidth to two 8-slot memory extenders. The I/O controller provides twelve 250MB/s data channels, for an aggregate bandwidth of 3.2GB/s distributed among the 10 PCI slots and multi-function core I/O.

The rp5430 architecture is similar to the rp5470. However, only half of the processor, memory, and I/O slot capacity is utilized.

figure 2.1 rp5470 architecture



low-latency memory access

Both the rp5430 and rp5470 support one or two 8-memory-slot carrier boards, for a maximum of 16 memory slots. The memory for both systems is connected to the CEC through a low-latency/high-bandwidth bus. With approximately half the latency of HP's previous generation K-Class server, the rp5400 series can supply the CPU with requested data in a fraction of the time of competitive systems.

The rp5400 series uses state-of-the-art synchronous dynamic random access memory (SDRAM) technology, available in 256MB, 512MB, 1GB, and 2GB DIMM pairs, all with advanced error checking and correcting (ECC) protection to detect and correct single-bit errors. The rp5470 supports up to 16GB of total system memory. The rp5430 supports up to 8GB of memory. Although all sixteen memory slots are active in the rp5430, the system will not boot if more than 8GB of memory is loaded. Memory configurations should be planned appropriately.

The "stretch" core electronics complex used in the rp5430 and rp5470 supports memory chip spare. This high-availability technology detects and corrects multiple-bit errors on memory DIMMs. With chip spare, any single DRAM chip can fail and the system will continue to operate normally. Chip spare is not supported on the 256MB DIMM pair, nor is it supported on the older-generation rp5400 and rp5450 servers.

6.255

To decrease memory latency and improve performance, the memory address lines are buffered three times: once on the system board to drive each memory carrier, once on the memory carrier to drive banks of DIMMs, and again on each DIMM before driving the memory components.

speeds and feeds

Tables 2.1 and **2.2** show the theoretical maximum bandwidth for various system buses. Theoretical maximum bandwidth is defined as the bus width multiplied by the frequency and number of buses.

table 2.1 maximum bandwidth for rp5470 system buses

	# of buses (or controllers)	maximum bus bandwidth	aggregate bus bandwidth
twin-turbo PCI slots	2	500MB/s	1GB/s
turbo PCI slots	6	250MB/s	1.5GB/s
shared PCI slots	1	250MB/s	250MB/s
core I/O	1	250MB/s	250MB/s
I/O subsystem	1 (controller)	3.2GB/s	3.2GB/s
memory subsystem	2	2.15GB/s	4.3GB/s
CPU buses	2	2.15GB/s	4.3GB/s

table 2.2 maximum bandwidth for rp5430 system buses

	# of buses (or controllers)	maximum bus bandwidth	aggregate bus bandwidth
twin-turbo PCI slots	2	500MB/s	1GB/s
turbo PCI slots	3	250MB/s	750MB/s
core I/O	1	250MB/s	250MB/s
I/O subsystem	1 (controller)	2.1GB/s	2.1GB/s
memory subsystem	2	2.15GB/s	4.3GB/s
CPU buses	2	2.15GB/s	4.3GB/s

I/O subsystem design

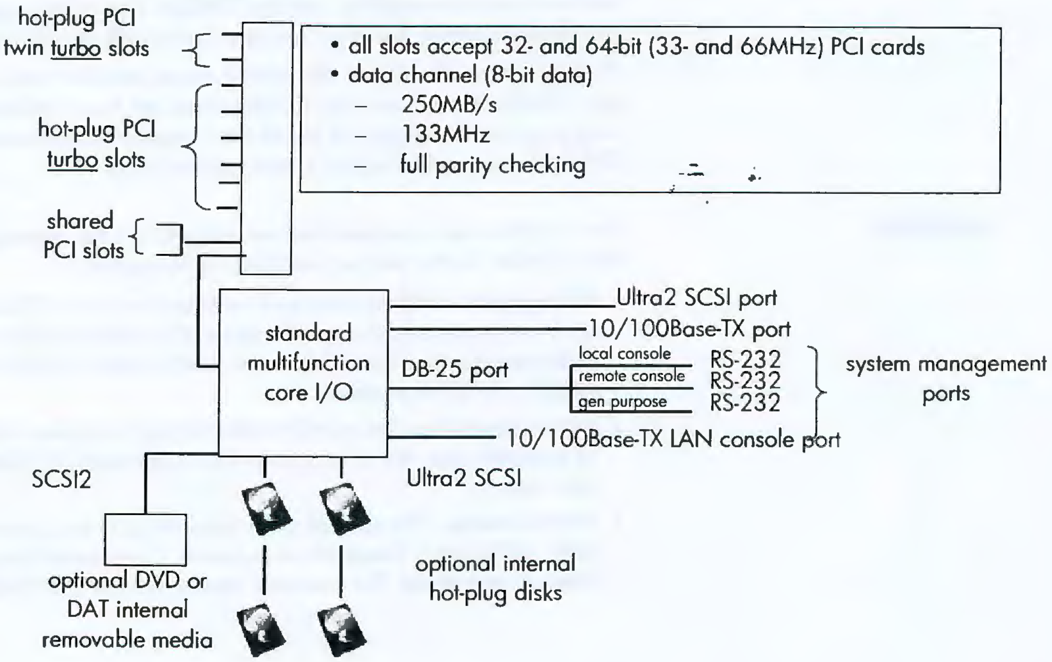
The rp5470 contains ten PCI I/O slots. The top eight slots have hot-plug capabilities under HP-UX 11i. The eight hot-plug slots all have independent I/O channels. This independent design prevents slow cards from affecting the performance of a fast card. Not only does independence provide great performance, but it also provides error containment. For example, if a card hangs slot 9, cards in slots 0–8 will still function properly. The first two hot-plug slots are twin-turbo slots, meaning they each have two dedicated 250MB/s channels or a total of 500MB/s per slot. These two slots should be reserved for the highest performing I/O cards, such as Fibre Channel, Gigabit Ethernet, or Hyperfabric controllers. The remaining six hot-plug slots are turbo slots, each with a single 250MB/s channel.

In addition to the eight hot-plug slots, the rp5470 has two shared PCI slots. These slots share a single 250MB/s channel.

All ten of the rp5470 I/O slots use HP-developed adaptive signaling technology to automatically match an I/O card's appropriate speed and data width. Therefore, all slots will accept 64- or 32-bit cards running at either 33MHz or 66MHz.

The rp5430 I/O subsystem is similar to the rp5470. In the rp5430, however, the shared PCI slots and three of the turbo slots are not active. Both twin turbo slots, four additional turbo slots, and the multifunction core I/O are available in the rp5430.

figure 2.2 **rp5470 I/O subsystem**



PCI is the optimized, industry-standard I/O bus. **Tables 2.3** and **2.4** summarize the PCI slots for each of the systems in the rp5400 series.

table 2.3 rp5470 PCI I/O

	# of slots	**hot plug**	**bandwidth per channel**	**bus width**	**signaling speed**	**slot keying**	**adaptive signaling**
twin turbo	2	yes	500MB/s	64 bits	66 & 33 MHz	5 volts	yes
turbo	6	yes	250MB/s	64 bits	66 & 33 MHz	5 volts	yes
shared	2	no	250MB/s	64 bits	33MHz	5 volts	yes

table 2.4 rp5430 PCI I/O

	# of slots	**hot plug**	**bandwidth per channel**	**bus width**	**signaling speed**	**slot keying**	**adaptive signaling**
twin turbo	2	yes	500MB/s	64 bits	66 & 33 MHz	5 volts	yes
turbo	4	3 of 4	250MB/s	64 bits	66 & 33 MHz	5 volts	yes

internal removable media

The rp5400 series contains a single removable media bay that can accommodate either a DVD-ROM or DDS-3. The media bay is supported by one of two SCSI controllers located within the core I/O.

A dedicated single-ended (SE) SCSI channel connects the media bay to the controller. The removable media bay does not support hot-plug capability. The DVD-ROM drive provides access of up to 650MB of data from one disk. The DVD-ROM drive provides enhanced features while preserving backward read compatibility with the CD-ROM. Data transfer rates of up to 6.75MB/s are achieved with the DVD format; 4.8MB/s can be achieved with the CD format.

The DDS-3 drive offered with the rp5400 series provides storage capacity of up to 12GB on a single tape. This drive can store up to 7.2GB of data per hour, and automatic read-after-write verification helps to ensure the integrity of stored data. Read-write backward compatibility with DDS-1 and DDS-2 allows continued use of existing archive tapes.

scalability

The rp5400 series is designed without tradeoffs in CPU, memory, internal storage, or I/O expandability to offer the best scalability in the market.

- **CPU upgrades**—With its entry-level configuration of one CPU and single-CPU increments available up to four processors, the rp5400 series offers great flexibility to cover a wide range of performance points. The rp5430 and rp5470 offer 875MHz PA-8700+ processors, as well as the 750MHz PA-8700 processor.
- **memory upgrades**—The rp5400 series memory subsystem is also designed for scalability. With 16 available slots, the servers range from a minimum of 256MB to a maximum of 16GB of main memory.
- **internal storage**—The rp5400 series supports up to four internal hot-plug disk drives, which can be either half-height or low-profile form factors. Current disk offerings include 18, 36, and 73GB Ultra160 disk drives. The maximum internal storage is 292GB, via four 73GB drives.

rp5400 series industrial design and packaging

The rp5400 series has been designed to fit into environments ranging from data centers to deskside. The industrial design is coordinated with other HP servers and peripherals for a consistent appearance.

racking density

The rp5400 series is designed to provide unprecedented performance density that easily adapts to different environments. At 7 EIA units (EIA unit= 1.75 inches), up to five rp5430 or rp5470 systems can be installed into a single 2-meter HP cabinet. With the high cost of computer room floor space, this small footprint dramatically lowers total cost of ownership.

The rp5400 series is supported in A490xA and A189xA cabinets. When using the high availability slider rail, bolt-on anti-tip feet are required. When using the slider in A189xA cabinets, ballasts are required (see the HP 9000 Enterprise Servers Configuration Guide for details).

The rp5400 series is also supported in a variety of third-party, non-HP racks and cabinets. Please refer to the HP 9000 Enterprise Servers Configuration Guide for the latest list of qualified third-party racks.

Note—dimensions for rack configuration: H= 12.25 inches (311 mm), D= 30.5 inches (775 mm), W= 19 inches (482 mm).

high availability slider rails

There are two rail options, static or slider, available for racking the rp5400 series into an HP cabinet. The high availability (HA) slider rails were designed to allow easy service access to the system, as well as to enable the hot-plug capability of the I/O slots and the hot-swap of four fans in the side cavity. With the HA slider rail, the rp5400 series can be completely serviced without removing it from the rack, thus allowing side-by-side racks of systems to be completely supported without sacrificing floor space for side access to the system. The slider rails also contribute to a 100% improvement in "mean time to repair" over D- and K-Class servers. The high availability slider rails are highly recommended.

Note—the slider mechanism occupies 1 EIA unit of rack space. When used with the rp5400 series, the combination will occupy 8 EIA units of rack space.

Static rails do not consume EIA space within the cabinet, therefore leaving more EIA space for peripherals. However, using static rails prohibits hot-plug of the I/O cards and hot-swap of the I/O bay fans.

cabinet spacing requirements

The rp5400 series requires a minimum of 24 inches (61 cm) of free space in both the front and rear of the cabinet for proper ventilation. During product installation and servicing, a total of 32 inches (82 cm) of free space is needed at the front of the cabinet.

The depth of HP A490xA cabinets is 39 inches (99 cm). Therefore, a minimum of 87 inches (221 cm) of total space is needed for each cabinet during normal operation. An additional 8 inches (21 cm) is needed during installation and servicing.

standalone/deskside configuration

The rp5400 series is also available in a standalone configuration when a cabinet is not desired. The standalone system is ideal for an office environment, under a desk, or on a shelf. The standalone configuration utilizes the same internal chassis and front plastic bezel as the racked version. However, a sheet metal cover, base, and casters are added for functionality and aesthetics. Casters can be removed when not desired.

Note—dimensions for standalone/deskside configuration: H= 14.5 inches (368 mm), D= 30.5 inches (775 mm), W= 19 inches (482 mm).

high availability

The rp5400 series has numerous high availability features that are unmatched in the entry-level server market—features such as redundant hot-swap fans and power, hot-plug I/O and disks, memory scrubbing and page deallocation, memory chip spare, independent PCI slots, failure avoidance and notification capability, and MC/Serviceguard support. These features improve the availability level of the total system and are introduced in this section.

redundant, hot-swap power supplies

HP power supplies have a long history of excellent reliability, and the redundant power supply option increases HP's commitment to even higher reliability and availability.

The rp5400 series power subsystem holds a maximum of three hot-swap power supplies. These supplies are located in the very front of the server. Each supply is capable of sustaining 930 watts of output. The rp5430 comes standard with one power supply; a second and even third supply can be added for N+1 or N+2 redundancy. The rp5470 comes standard with two power supplies; a third supply can be ordered for N+1 redundancy. Each power supply has its own power cord, which provides protection against losing the power from a single cord or breaker. To maximize availability, the power cords should be plugged into separate breakers whenever possible.

Because of the hot-swap capability, in the event of a power supply failure, the faulty supply can be removed and replaced without notifying the system. This, of course, is assuming that an N+1 condition exists.

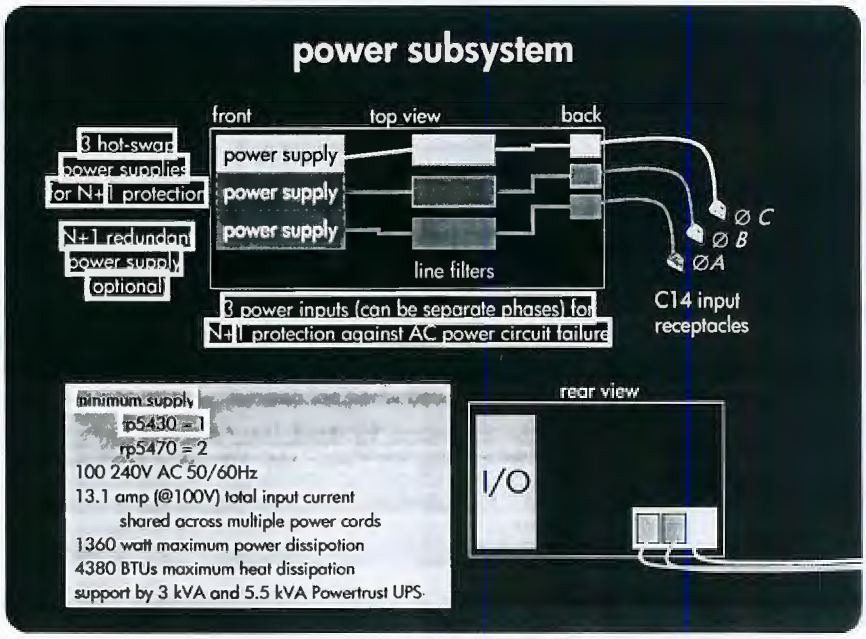
Exchanging a power supply in a running system involves opening the hinged, front plastic bezel. The failed power supply is easily identified and removed. The power supply is exchanged with a good one and the door is then closed to finish the process. The system will log a management code to indicate that redundancy is re-enabled. It is that simple.

There is another advantage for those customers with rigorous preventative maintenance programs. While the server continues to operate, the power supplies can be removed one-at-a-time and dust buildup can be vacuumed using proper electrostatic discharge (ESD) procedures.

redundant power input protection

Figure 3.1 contains a diagram of the rp5400 series power subsystem. This section explains how customers can utilize these capabilities to achieve different levels of power input protection.

figure 3.1 power subsystem



power subsystem
front
top view
back
3 hot-swap power supplies for N+1 protection
N+1 redundant power supply (optional)
power supply
power supply
power supply
line filters
Ø C
Ø B
ØA
C14 input receptacles
3 power inputs (can be separate phases) for N+1 protection against AC power circuit failure
rear view
I/O

minimum supply
rp5430 = 1
rp5470 = 2
100 240V AC 50/60Hz
13.1 amp (@100V) total input current
shared across multiple power cords
1360 watt maximum power dissipotion
4380 BTUs maximum heat dissipation
support by 3 kVA and 5.5 kVA Powertrust UPS.

The server has three AC input line cords to reduce single points of failures. Each line cord supplies power to one of the three internal power supplies. The system is designed to operate on nominal 100–240 VAC and 50- or 60-Hz power without line-select switches. Each power supply can draw up to 930 watts. Because the servers will continue to operate with two of the three supplies functioning, many possibilities exist for the customer to configure the AC input depending on the level of protection desired. If the site has very stable AC power, all three line cords could be plugged into the same power grid. For additional protection, a single uninterruptible power supply (UPS) could be utilized to supply power to all three cords if primary AC power should fail.

- The next higher level of protection is to have three branch AC circuits, one for each AC input. This reduces the dependency on single-point breaker failures and common wiring. Additional protection for this configuration would utilize three smaller UPSs.
- The highest level of protection is three electrical utilities that each supply a branch circuit. This approach is expensive but does greatly reduce single points of failures. Large sites with many systems may find this configuration cost-effective. For the ultimate protection of large sites, install a large UPS on each branch circuit.

redundant, hot-swap cooling

The rp5400 series contains eight hot-swappable fans to cool system components. The eight cooling fans (1 front-access, 4 side-access, 3 rear-access) are arranged in an N+1 configuration so any fan can fail and not affect system uptime. In the event of a fan failure, the faulty fan can simply be removed and replaced while the server continues to run. The design pairs fans together. If one fan fails, the other speeds up to ensure adequate system cooling.

In addition, the server monitors ambient temperature and the power consumed within the box to determine the desired fan speed. By sensing the tachometer outputs from each fan, the actual speed is determined. Digital phase locked loop (DPLL) circuitry is used to individually adjust the speed of each fan to the desired common speed.

These smart algorithms reduce unnecessary fan noise, power consumption, and wear while producing a very clear indication of a working, cooling subsystem. In the unlikely event of a fan failure, it will drop out-of-lock with the DPLL. The server signals a fan failure via chassis codes to the console and will light an LED on the failed fan assembly.

There is another advantage for those customers with rigorous preventative maintenance programs. While the server continues to operate, the fans can be removed one-at-a-time and dust buildup can be vacuumed using proper ESD procedures.

main memory—advanced ECC and parity

Data stored in the main memory is protected by error checking and correcting (ECC) and address/control parity. The ECC design provides memory scrubbing and page deallocation functionality that will tolerate typical hard single-bit SDRAM failures without requiring DIMM replacement.

The data controllers generate ECC bits and store these ECC bits with the data in the DIMMs. The 256MB, 512MB, and 1GB DIMMs use x4 SDRAMs to store each bit of a word, including its ECC bits, in a different SDRAM within the DIMM pair. The 128MB DIMMs use x8 SDRAMs. When reading the data back, the data controllers are able to detect and correct single-bit data errors. Double-bit errors cannot be corrected. Double-bit data errors are highly unlikely because the data and ECC bits are stored one-bit-per-SDRAM, and multiple SDRAMs would have to be involved in the error. Hence, a single SDRAM could fail within each DIMM pair and the system would still function.

The system also detects address and control parity errors to prevent data corruption from reading or writing to the wrong location in main memory. The address controller and each address buffer generate address and control parity. Each address buffer detects address and control parity problems and reports it back to the address controller. There are three levels of address buffers as the address lines fan out. These address buffers are located on the system board and on each memory carrier on each DIMM.

memory chip spare technology

Chip spare is the ability of the system to continue to run in the face of any single or multi-bit chip error on a DRAM. DRAMs are basically N+1 per memory word. This functionality is essential in the design of reliable memory systems. Systems without this functionality are doomed to fail at an alarming rate when compared to HP servers.

Both the rp5430 and rp5470 support chip spare. The 256MB DIMM pair (product A5554A) does not support chip spare. To ensure maximum memory availability, the rp5430 and rp5470 should be configured with 512MB, 1GB, or 2GB memory modules only. The older generation rp5400 and rp5450 do not have chip spare capabilities.

hot-plug disk drives

The rp5400 series has four embedded SCSI disks accessible from the front of the server. These disks can be removed and inserted while the server continues to operate. This operation is called hot-plug, and it is different from hot-swap.

During both hot-plug and hot-swap operations, the power remains on and the system continues to function. However, hot-swap means that the assembly can be removed, added, or replaced without informing the system. Hot-plug requires the assembly to be deconfigured before removal and reconfigured before the system can utilize the newly inserted assembly. Because disks have unique information stored on them, hot-plug methods are used. Fans and power supplies are hot-swap assemblies.

Two dual-channel SCSI controllers manage the four internal hot-plug disks. For added availability, disk pairs are on separate channels as well as separate SCSI controllers. This means that with disk mirroring, a SCSI controller, SCSI channel, or root disk could fail and the server would continue to run properly.

The rp5400 series contains circuitry to properly control the disk's power and reset during the hot-plug operation. Either system administration manager (SAM) or the MESA suite of online diagnostic software can be utilized to effectively deconfigure and reconfigure the disk.

Another advantage for those customers with rigorous security programs is the ability to completely remove and isolate disks in a disaster- and theft-safe environment.

hot-plug PCI I/O slots

The ability to hot-plug PCI cards offers excellent flexibility for adding, reconfiguring, and maintaining I/O functions while the system continues operations. No reboot is required.

The I/O card bay is located at the right rear of the chassis. The I/O bay supports up to 10 PCI cards. Access to the I/O bay in rackmounted systems utilizing the high availability slider is achieved by sliding the server forward. Special features on the chassis, along with custom rack rails, allow the unit to move safely and smoothly during online service with all cables still attached. Once the system is slid into the service position, the I/O bay cover can be removed to gain side access to the PCI cards. In the standalone configuration, the outer shell is removed to gain access to the I/O bay.

The rp5470 has ten PCI I/O slots, and eight of those slots are hot-plug capable. Each hot-plug slot supports 64-bit × 66MHz PCI cards running at full speed and is connected to the I/O controller via independent, high-speed 250MB/s channels. This independent design prevents slow cards from affecting the performance of a fast card. Not only does independence provide great performance, but it also provides error containment. For example, if a card hangs in slot 10, cards in all other slots will still function properly. The highest-performing cards should always be placed in these independent slots.

The rp5430 has six PCI I/O slots. Ten physical slots are available, but only six of the slots are functioning electrically. Five of these six slots support hot-plug actions.

The PCI cards are spaced on a .9-inch pitch to allow for special hot-plug features and increased PCI reliability. Extra airflow holes between bulkheads more than double PCI airflow. Between the PCI slots, I/O card separators prevent electrical shorting and exposure to hazardous energy during hot-plug installation and removal. Locking features are designed into the main chassis to eliminate the need for individual PC board bulkhead screws, thus removing a potential electrical safety hazard.

Hot-plugging I/O cards have both hardware and software components. The hardware requirements are met by the electronics on the I/O backplanes and by mechanical design in the I/O cardcage. Bus idling, slot-to-slot electromechanical isolation, per-slot power and reset control, and visual indicators are all components of the total hot-plug hardware solution. With associated software, any card located in a hot-pluggable PCI slot can be removed, replaced, or added without power cycling, rebooting the system, or impacting the operation of other I/O transactions.

Please note that software support for hot-plug I/O is available in HP-UX 11i, but not in HP-UX 11.0.

dynamic processor deallocation and resilience

Every multi-CPU server with properly loaded HP-UX 11 has the capability for Dynamic Processor Deallocation and Resilience. Incorporated into HP-UX 11 is the capability to take a processor out of service while the system is running, without interruption to applications. This technology is referred to as Dynamic Processor Deallocation. Once a processor is deallocated, the HP-UX operating system will migrate all application processes that are currently scheduled on that processor to other active processors. Note that if the processor has been assigned to handle interrupts for any I/O drivers, it will continue to do so while it is deallocated.

The rp5400 series PA-RISC processors have the ability to detect and correct single-bit cache errors. The embedded event monitoring service (EMS) monitors the rate of correctable errors in each processor's on-board cache. These errors are manifested as low-priority machine checks (LPMCs). While occasional correctable errors are to be expected in the on-board cache, too many of these errors in a short period of time indicate an increased likelihood that a non-correctable cache error could occur. The EMS LPMC monitor will continuously monitor the rate at which LPMCs are occurring and dynamically deallocate a processor, using the Dynamic Processor Deallocation facility. This technology is referred to as Dynamic Processor Resilience.

manageability and support

The rp5400 series has many features to minimize the effort required to manage one system or an entire computer room. The server simplifies system management in several aspects: event notification, automatic error handling, power monitoring, and user interface to system management.

LED event notification

For an operator who is physically present, the simplest and easiest way to check system status is by quickly glancing at the status LEDs on the front of the system. The five LEDs each have a specific meaning:

- power—power is present and on, and power supplies are functioning properly
- remote—remote console is enabled
- run—system is up and running
- attention—occurrence of a non-catastrophic event, e.g., failure of an N+1 component
- fault—occurrence of a catastrophic system event

In addition to the five specific meanings of the LEDs, related system status is encoded based on whether the LED is solid or flashing. Examples include unexpected reboot system recovered, operating system not running, and operator intervention required.

event monitoring service

HP EMS is a system monitoring application designed to facilitate remote/centralized real-time monitoring and error detection for HP products in the enterprise environment. This framework provides centralized management of hardware devices such as the rp5400 series servers and system resources, and it provides immediate notification of hardware failures and system status. HP EMS can receive data on unusual activity, add information on the problem's source, and provide recommendations on problem resolution.

HP EMS consists of a set of system and network monitors within a monitoring environment. This monitoring framework has an easy-to-use interface and provides a mechanism for monitoring resources, registering monitoring requests, and sending notification when resources reach user-defined critical values.

How it works:

- A hardware event monitor detects abnormal behavior in one of the hardware resources (devices) it is monitoring.
- The hardware event monitor creates the appropriate event message, which includes suggested corrective action, and posses it to the EMS.
- EMS sends the event message to the system administrator using the notification method specified in the monitoring request (for example: e-mail, message to the console, entry in a system log).
- The system administrator (or HP service provider) receives the message, corrects the problem, and returns the hardware to its normal operating condition.
- If the peripheral status monitor (PSM) has been properly configured, events are also processed by the PSM. The PSM changes the device status to DOWN if the event is serious enough. The change in device status is possed to EMS, which in turn alerts MC/Serviceguard. The DOWN status will cause MC/Serviceguard to failover any package associated with the failed hardware resource.
- Any of the following consoles can be used with EMS to remotely monitor server farms: HP MC/Serviceguard, CA Unicenter, HP OpenView ITO, HP Secure Web Console, and HP Toptools.

The monitors can also poll hardware, disks, clusters, network interfaces, and system resources and send information to the framework. An "event" can be simply defined as something you want to know about—for example, a disk failure or file space dropping below a predefined level.

The primary EMS benefits include:

- enables efficient and effective system monitoring within a single, comprehensive framework
- delivers the ability to tailor the monitoring system to fit specific needs

- provides a wide variety of notification methods through multiple protocols (SNMP traps, TCP, UDP, OPC messaging)
- provides immediate alerts if a component fails, enabling proactive replacement
- integrates with HP MC/Serviceguard and Serviceguard OPS Edition to provide a complete high-availability solution

extended fault management system

The rp5400 series employs a dedicated processor to aid system management and diagnosis. The extended fault management system can diagnose a system failure even in the unlikely event that the system is unable to execute code. It allows system power to be remotely turned on or off, and it has battery backup that even allows diagnosis of power failures. The system interfaces with key components via an inter-integrated circuit (I^2C) bus to continually monitor the status of system fans, temperature, and power supplies; it signals the operator if any significant system events occur.

Major features of the extended fault management system include:

- system console redirection
- console mirroring
- configuration of system for automatic restart
- viewing history log of system events
- viewing history log of console activity
- setting inactivity timeout thresholds
- remote system control
- power control—remote power on and off
- viewing system status logs
- configuration of virtual front-panel display
- event notification to system console, e-mail, pager, and/or HP Response Centers
- auto system restart
- virtual front-panel display
- password security (same level as UNIX)

system platform monitor

Closely integrated with the extended fault management system is the system platform monitor. The system platform monitor controls and monitors system power and cooling. Aspects controlled and monitored by the system platform monitor are:

- power supply status and temperature
- system supply voltages—including remote system power on and off
- total system power consumption
- individual Processor Support Module status
- external ambient air temperature
- individual fan speed and status

Various temperatures are monitored to control the system fans, provide thermal warnings, and prevent permanent damage from overheating by graceful shutdown if the temperature is too high. (Note that the system fans are run only as fast as necessary to keep the system cool. The fans are kept in sync with each other, turning at exactly the same rate. This intelligent fan control allows the L-Class to generate as little noise as possible while maintaining an optimum operating environment to maximize reliability.)

The power monitor senses the presence of power supplies and the power consumption of system components to determine if the system is in an N or N+1 power configuration; it can determine:

- number of bulk power supplies
- number of CPUs
- amount of memory present
- number and power consumption of each installed PCI I/O card

System configuration and health is tracked by the system platform monitor and passed via a dedicated I^2C bus to the fault management processor. This information can be processed as follows: simply displayed on the system console, logged to an event file, or used to trigger an alert based on a specific threshold (system temperature, fan status, or power supply status, for example).

built-in Web console

The rp5400 series has integrated Web console functionality, which allows management of many systems from a single Internet browser. The Web console is embedded into the fault management processor and can be accessed through the core 10/100Base-TX management LAN. The external Secure Web Console box that shipped with older-generation HP servers is no longer needed. The Secure Web Console allows an Internet browser to be used as a system console, giving total system access to authorized system administrators anywhere, just as if they were at an ASCII console. A high level of password protection is used to control access to the Web console.

Major features of Secure Web Console include:

- system management over the Internet or intranet
- mirrored access—up to four operators can simultaneously share the same screen and keyboard
- security—built-in password encryption, data scrambling, and Java™ download protection
- universal browser-based support for Netscape v.3.0+ and Microsoft® Internet Explorer v.3.0+ Web browsers
- easy updates of Web console software over the network
- easy installation—just connect the L-Class console part to a LAN; there is no client software to install
- support for HTTP, FTP, TFTP, and other key Internet standards

LAN console

The server also provides a LAN console interface using industry-standard telnet connections. Like the Web console, the LAN console can be used remotely for managing many systems from a single control center. The telnet interface allows scripts to be used to vastly simplify multiple system management. Password protection provides a high level of security to control access to the LAN console, ensuring that only authorized personnel perform system management.

ASCII consoles

For users who wish to locally administer their systems, the rp5400 series provides an RS-232 part to use for ASCII terminal console connections. Any VT100-capable terminal or emulator can be used as a local system console.

remote access

As with previous HP server systems, an RS-232 interface for a remote console is useful for obtaining help from HP service experts. Customers need only add a modem to allow remote access via phone; security is ensured by having to explicitly enable remote console access, which is protected with a password, and via dial-back phone verification.

self-diagnosis

Many features have been designed into the server to maximize system uptime. There are several aspects to maximizing uptime: eliminating common single points of failure, allowing the system to continue running after some errors, and allowing quick identification and servicing of hardware faults if they do occur.

Besides using traditional diagnostic software, the server also continuously monitors system health with the platform monitor. Knowing a failure has occurred that reduces N+1 protection is important. It is important to minimize the risk of downtime by replacing a failed component as soon as possible to get back to the safety of an N+1 configuration. To enable this, the server provides several methods of event notification.

The rp5400 series has extensive firmware-based self-tests. These diagnostics are evoked on power-up or reset. The self-tests check for correct system operation prior to booting the operating system. The firmware diagnostics first check the processors, then processor caches and memory, and finally I/O devices. Testing complexity increases as more of the system is proven good and more pieces of the system can be relied upon to increase test coverage on the remaining parts. Self-test failures are reported to the system console and the support processor, along with failure specifics and recommended corrective action.

online and offline diagnostics

The rp5400 also offers traditional online and offline diagnostics to validate system health and provide extensive system fault coverage.

With online diagnostics, the system is tested while the operating system and applications continue to run. This allows basic testing of system components that are not currently being used, or it allows testing in situations where the testing does not prevent continued use of the operating system and applications.

Offline diagnostics provide increased coverage of system components for improved fault isolation and intensive system testing before returning to production.

6243
2

for more information

HP product information and technical documentation is available online at:

http://www.hp.com/go/rp5430

http://www.hp.com/go/rp5470

Contact any of our worldwide sales offices or HP Channel Partners (in the U.S., call 1-800-637-7740) or at the following international numbers:

United States of America:
+1 800 637 7740
Canada:
Hewlett-Packard Ltd.
5150 Spectrum Way
Mississauga, Ontario L4W 5G1
+1 905 206 4725
Japan:
Hewlett-Packard Japan, Ltd.
Japan Country H.Q.
3-29-21, Takaido-Higashi, Suginami-ku,
Tokyo, 160-8585 Japan
+81 3 3331 6111
Latin America:
Hewlett-Packard
Latin American Region Headquarters
Waterford Building, 9th Floor
5200 Blue Lagoon Drive
Miami, Florida 33126 USA
+1 305 267 4220
Refer to country phone numbers
Australia/New Zealand:
Hewlett-Packard Australia Ltd.
31-41 Joseph Street
Blackburn, Victoria 3130
Australia (A.C.N. 004 394 763)
+61 3 9272 2895
Asia Pacific:
Hewlett-Packard Asia Pacific Ltd.
17-21/F, Shell Tower
Times Square
1 Matheson Street
Causeway Bay
Hong Kong
+8522 599 7777
Europe/Africa/Middle East:
Hewlett-Packard S.A.
150, Route du Nant-d'Avril
CH-1217 Meyrin 2
Geneva, Switzerland
+41 22 780 81 11
European Multicountry: +41 22 780 81 11
Middle East and Africa: +41 22 780 71 11
European Headquarters: +41 22 780 81 81

For direct country contact call:
Argentina: +541 787 7145
Austria: +43 1 25 000 0
Belgium and Luxembourg: +32 2 778 31 11
Brazil: +5511 7296 8000
Chile: +562 203 3233
Colombia: +571 629 5030
Denmark: +45 45 99 10 00
East Central Europe, CIS, and Yugoslavia:
+43 1 25 000 0
Finland: +358 9 887 21
France: +33 1 69 82 60 60
Germany: +49 7031 140
Greece: +30 1 689 644
Hungary: +36 1 252 7300
Iceland: High Performance Systems hf.
+354 1 67 10 00
Ireland: +353 1 615 8200
Israel: Computation and Measurement Sy
(CMS) Ltd. +972 3 5380 333
Italy: +39 2 92122770
Mexico: +525 326 4600
Netherlands: +31 20 547 6911
Norway: +47 22 7356 00
Poland: +48 22 608 77 00
Portugal: +351 1301 7343
Russia and the CIS, excl. Ukraine:
+7 095 923 5001
Slovenia: +38 61 55 84 72
Spain: +34 1 631 1600
Sweden: +46 8 444 2000
Switzerland: +411 735 7111
South Africa: Hewlett-Packard South Africa
(Pty) Ltd.+27 11 806 785 1000
Turkey: +90 212 224 5925
United Kingdom: +44 1344 369231
Venezuela: +582 239 4133

Technical information contained in this document is subject to change without notice.

08/02
5981-2650EN

Apêndice EF

CISCO SYSTEMS

CiscoWorks **VPN/Security Management** Solution Version 2.2

CiscoWorks VPN/Security Management Solution (VMS) is the flagship integrated security management solution from Cisco, and is an integral part of the SAFE Blueprint from Cisco for network security. CiscoWorks VMS protects the productivity and reduces operating costs for enterprises, by combining Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network and host-based intrusion detection systems (IDS). CiscoWorks VMS delivers the industry's first robust and scalable foundation and feature set that addresses the needs of small and large-scale VPN and security deployments.

Today's business challenges and resulting security deployments require more scalability than merely supporting a large number of devices. Many customers have limited staffing, yet are asked to manage a myriad of security devices. These customers must manage the security and network infrastructure; frequently update many remote devices; implement change control and auditing when multiple organizations are involved in defining and deploying policies; enhance security without adding more headcount; or roll out remote access VPNs to all employees and monitor the VPN service.

CiscoWorks VMS enables customers to deploy security infrastructures from a small to large environment, using the following multifaceted scalability features:

- Complete SAFE Blueprint Coverage

  To completely manage a SAFE environment, a network management solution must manage SAFE infrastructure components, support features based upon an appliance or Cisco IOS® Software, and support a range of management functions. CiscoWorks VMS is uniquely able to scale across SAFE Blueprint components, including firewalls, VPNs, and network- and host-based IDSs. CiscoWorks VMS also takes advantage of Cisco Secure Access Control Server (ACS) by using a common ACS logon. CiscoWorks VMS can manage a feature set through an appliance, for example, the Cisco PIX® Firewall, or through the Cisco IOS Software. Scalable management also involves more than configuring devices. CiscoWorks VMS provides the complete range of management with features to configure, monitor, and troubleshoot the network.

- Scalable Foundation

  CiscoWorks VMS implements a foundation with a consistent user experience, which makes it easier to scale management to many devices. CiscoWorks VMS provides users with a consistent GUI, workflow, ACS logon roles definition, platforms, database

Cisco Systems, Inc.

engine, installation, and more. An industry-leading feature of this foundation is the Auto Update feature, which allows numerous devices to be updated easily and quickly. Auto Update enables devices, even remote and dynamically addressed devices, to periodically "call home" to an update server and "pull" the most current security configurations or Cisco PIX operating system. Auto Update is required to effectively scale remote office firewall deployments across intermittent links or dynamic addresses. Prior policy updating methods relied on a "push" model. Although this model works for known devices, it does not work for remote devices with unknown addresses or devices that are not always active. Without Auto Update a more manual process is required to update each remote device. The Auto Update feature provides a dramatic scalability improvement for organizations that want to deploy devices with many remote and local locations. In addition to easier and faster policy updates, Auto Update also provides consistent policy deployments.

- Enterprise Operational Integration

  CiscoWorks VMS enables organizations to easily integrate management into their operations. One operational need is to replicate policies to multiple locations. The Smart Rules hierarchy addresses this need, by enabling administrators to define device groups and implement policy inheritance. For example, an administrator can define a device group for the New York sales office and deploy that same policy to all other sales offices quic and consistently. The Command and Control Workflow feature provides change control and auditing, and is particularly important for customers who have separate groups for network and security operations. The solution includes processes for generating, approving, and deploying configurations. This can help security operations to define and approve new policies. Network operations can later deploy the new policies during their regular maintenance window. An audit of the changes can be maintained.

- Centralized Role-Based Access Control (RBAC)

  Role-based access control enables organizations to scale access privileges. CiscoWorks VMS conveniently uses a common ACS logon for users, administrators, devices, and applications. CiscoWorks VMS enables different groups to have different access rights across different devices and applications.

- Integrated Infrastructure Management

  Scalability requires that multiple components be managed, not just firewalls, but also VPNs, network- and host-based IDSs, routers, and switches. CiscoWorks VMS not only manages the security infrastructure, but also manages the network infrastructure. Customers benefit from being able to manage these components from one solution. Integrated monitoring is also required to see the larger picture. CiscoWorks VMS provides integrated monitoring of Cisco PIX and Cisco IOS syslogs, and events from network and host-based IDSs, along with event correlation.

CiscoWorks VMS Functions

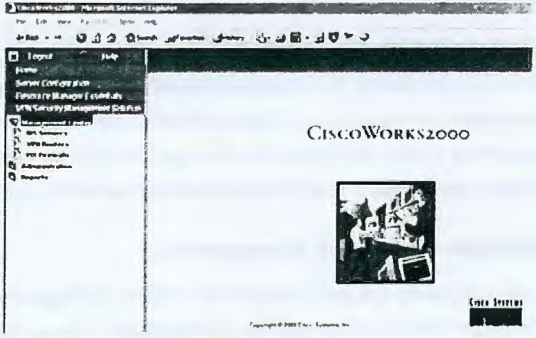
CiscoWorks VMS is launched from the CiscoWorks dashboard and is organized into several functional areas:

- Firewall management
- Auto Update Server
- IDS management, network and host-based
- VPN router management
- Security monitoring
- VPN monitoring
- Operational management

These functional areas supply multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control.

Figure 1 shows CiscoWorks VMS displayed as a "drawer" in the CiscoWorks dashboard.

Figure 1



Firewall Management

CiscoWorks VMS enables the large-scale deployment of Cisco PIX firewalls, by providing the following features:

- Smart Rules hierarchy and inheritance
- User-defined device and customer groups including nesting
- Global role-based access with administrative privileges per device and customer groups with other CiscoWorks products and Cisco Secure ACS
- Mandatory and default device settings inheritance
- Workflow deployment to device, directory, or Auto Update Server
- Look and feel of Cisco PIX Device Manager but with scalability to thousands of PIX firewalls
- Integration with other CiscoWorks network management software
- Complete SAFE Blueprint coverage for centralized management of Cisco PIX firewalls, including access control, VPN, IDS, and authentication, authorization, and accounting (AAA)

Smart Rules is an innovative feature that allows common information including access rules and settings to be inherited for all firewalls in a device or customer group. Smart Rules allows a user to define common rules once, which results in reduced configuration time, fewer administrative errors, and higher device scalability. Using Smart Rules, a user can configure a common rule such as allowing all HTTP traffic once and can apply this rule globally to all firewalls. Smart Rules can also be defined on a device or customer group basis. For specific information on the firewall management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3992/index.html

Auto Update Server for Firewall Management

CiscoWorks VMS introduces the industry's first firewall Auto Update Server that allows users to implement a "pull" model for security and Cisco PIX operating system management. Auto Update Server permits remote firewall networks with unprecedented scalability. The Auto Update Server allows Cisco PIX firewalls to both periodically and automatically contact the update server for any security configuration, Cisco PIX Operating System, and PIX Device Manager (PDM) updates. The Auto Update Server supports the following features:

- Security management of remote Cisco PIX firewalls that use Dynamic Host Control Protocol (DHCP)
- Automated Cisco PIX OS distribution to groups of Cisco PIX firewalls
- Automated Cisco PDM updates to remote firewalls
- Configuration verification at periodic intervals
- Automated replacement of inaccurate or tampered configurations
- New firewalls configured at "boot time"

The Auto Update Server is an indispensable component of any large-scale remote Cisco PIX firewall deployment. Auto Update Server is an easy-to-use solution to automatically update all remote or local firewalls with new operating system releases. Cisco is the industry's first vendor to provide this pull model of security policy and operating system management. For specific information on the Auto Update Server component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3993/index.html

Network-Based IDS Management

Administrators can use CiscoWorks VMS to configure network and switch IDS sensors. Many sensors can be quickly configured using group profiles. Additionally, a more powerful signature management feature is included to increase the accuracy and specificity of detection. Some prominent features are:

- Easy-to-use Web-based interface
- Wizards that lead users through common management tasks
- Access to the Network Security Database (NSDB), which provides meaningful information about alarms for users without IDS security expertise
- Ability to define a hierarchy of sensors containing groups and subgroups, and the ability to configure multiple sensors concurrently using group profiles
- Support for several hundred sensor deployments from each console
- Use of a robust relational database to store a high volume of data

For specific information on the network-based IDS management functionality of VMS, refer to:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

Host-Based IDS Management

CiscoWorks VMS provides threat protection for server and desktop computing systems, also known as "endpoi VMS goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications. Because CiscoWorks VMS analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs. Features of host-based IDS management include:

- Aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent.
- Provides preventive protection against entire classes of attacks including port scans, buffer overflows, Trojan horses, malformed packets, and e-mail worms.
- Offers "zero update" prevention for known and unknown attacks

- Provides industry-leading protection for UNIX and Windows servers and Windows desktops allowing customers to patch systems on their own schedules.
- Open and extensible architecture offers the capability to define and enforce security according to corporate policy.
- Scalable to thousands of agents per manager to support large enterprise deployments.

For specific information on the host-based IDS management functionality of VMS, refer to: the Management Center for Cisco Security Agents Datasheet.

VPN Router Management

CiscoWorks VMS includes functions for the setup and maintenance of large deployments of VPN connections and provides users with a point-and-click interface for setting up and deploying connections. This application is intended for scalable configuration of site-to-site VPN connections in a hub-and-spoke topology for centralized, multidevice configuration and deployment of Internet Key Exchange (IKE) and IP Security (IPsec) tunneling policies on VPN routers.

Major features include:

- Wizard-based interface for the creation of IKE and VPN tunneling policies.
- Hierarchical inheritance and Smart Rules hierarchy to reflect the organizational and common setup of devices and simplified device management
- IKE-KA (IKE Keepalive) or generic routing encapsulation (GRE) with Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) for failover routing scenarios.
- Centralized role-based access control model allows for centralized management of users and accounts.

For specific information on the VPN router management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3994/index.html

Security Monitoring

CiscoWorks VMS provides integrated monitoring to reduce the number of security monitoring consoles, reduce the number of events to monitor, and provide a broader view of security status.

- Integrated monitoring is used to capture, store, view, correlate, and report on events from many of the devices in the SAFE Blueprint such as Cisco network IDSs, switch IDSs, host IDSs, firewalls, and routers.
- Event correlation is used to identify attacks that are not easily recognizable from a single event. A flexible notification scheme and automated responses to critical events also aid in quick action.
- The event viewer can read both real-time and historical events.
- Events are color-coded and administrators can quickly isolate problems. Administrators can also define thresholds and time periods when rules can be triggered to provide notification.
- On-demand and scheduled reports facilitate ongoing monitoring.

For specific information on the security monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3991/index.html

VPN Monitoring

CiscoWorks VMS offers a Web-based management tool that allows network administrators to collect, store, and view information on IPsec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser. This dashboard provides the following capabilities:

- Provides data on system resources related to real-time memory usage, percent CPU usage per device, and active tunnel and active sessions. This data simplifies the identification of devices with potential performance problems and devices with the highest usage.
- Enables viewing of current and long-term packet rates and packet dropped percentage which can aid in determining where excess capacity can be tapped or quickly identify bottlenecks and device throughput problems.
- Enables identification of the devices with the most persistent problems through the event log; key device and VPN statistics are evaluated against a set of global and device-specific thresholds, and exceptions are recorded in the event log.
- Provides graphing of important common metrics. Device performance comparisons provide a global view of short-term trends in VPN performance, enabling administrators to identify problem areas before they become critical failures.

For specific information on the VPN monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2326/index.html

Operational Management

CiscoWorks VMS provides the operational management for the network, allowing network managers to perform the following:

- Quickly build a complete network inventory
- Manage device credentials information
- Monitor and report on hardware, software, configuration, and inventory changes
- Manage and deploy configuration changes and software image updates to multiple devices
- Monitor and troubleshoot critical LAN and WAN resources
- Quickly identify devices that can be used for VPNs, if upgraded with the appropriate Cisco IOS Software
- Discover which VPN devices have hardware encryption modules
- Graphically compare configurations of VPN devices
- Isolate IPsec-related problems by running customized Syslog reports

For specific information on the operational management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/index.html

Server Specifications (Minimum requirements)

Server Hardware

- PC-compatible computer with 1 GHz or faster Pentium processor
- Sun UltraSPARC 60 MP with 440 MHz or faster processor
- Sun UltraSPARCIII (Sun Blade 2000 Workstation or Sun Fire 280R Workgroup Server)

- CD-ROM drive
- 100BASE-T or faster connection
- 1 GB RAM
- 9 GB available disk drive space
- 2 GB virtual memory
- Color monitor with video card capable of 16-bit color

Server Operating System

CiscoWorks VMS requires the following operating systems:

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3)

Note: Support for Advanced Server requires that Terminal Services be turned off.

Sun Solaris 2.8 with patches:

109742 has been replaced by 108528-13

109322 has been replaced by 108827-15

109279 has been replaced by 108528-13

108991 has been replaced by 108827-15

Java Requirements

Sun Java plug-in 1.3.1-b24

Client Requirements

Hardware

- PC-compatible computer with 300 MHz or faster Pentium processor
- Solaris SPARCstation or Sun Ultra 10

Client Operating System

- Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM.
- Solaris 2.8

Client Browser

- Internet Explorer 6.0 Service Pack 1, on Windows operating systems
- Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP; Netscape Navigator 4.76 on Solaris 2.8

The CiscoWorks Management Center for Firewalls, and CiscoWorks Management Center for VPN Routers, are supported on Internet Explorer 6.0, but not on Netscape Navigator. In addition to supporting Internet Explorer The Management Center for IDS and the Monitoring Center for Security are also supported on Netscape Navigator.

Service and Support

CiscoWorks products are eligible for coverage under the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 24-hour access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A SAS contract ensures that customers have easy access to the information and services needed to stay current with newly supported device packages, patches, and minor updates. For further information about service and support offerings, contact your local sales office.

Ordering Information

CiscoWorks VMS is available for purchase through regular Cisco sales and distribution channels worldwide. CiscoWorks VMS includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris workstation.

For More Information

For more information, go to http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/ or send e-mail to ciscoworks@cisco.com

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice EG

CISCO SYSTEMS

Data Sheet

Cisco IDS 4200 Series Sensors

Cisco integrated network security solutions enable organizations to protect productivity gains and reduce operating costs.

The Cisco IDS 4200 Series sensors are used in the Cisco Intrusion Protection System. These intrusion detection system sensors work in concert with the other components to efficiently protect your data and information infrastructure. With the increased complexity of security threats, achieving efficient network intrusion security solutions is critical to maintaining a high level of protection. Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.

Additionally, Cisco's flexible deployment options allow businesses to minimize the total cost of ownership of their IDS deployments by delivering:

- unprecedented price/performance ratios
- the ability to simultaneously protect multiple network subnets through the support for multiple sniffing interfaces, thereby delivering up to five sensors in one
- a wide array of performance options
- investment protection by delivering modular, upgradable components
- support for multi-VLAN traffic
- embedded web-based management solutions packaged with the IDS sensors

Please refer to Table 1 for information on the characteristics of the Cisco IDS 4200 Series Sensors.

For details on the complete Cisco Intrusion Protection System, go to http://www.cisco.com/go/ids.

Deploying the Cisco IDS 4200 Series Sensors

The Cisco IDS 4200 Series includes four products: the Cisco IDS 4215, IDS 4235, IDS 4250 and IDS 4250-XL sensors. The Cisco IDS product line delivers a broad range of solutions that allow easy integration into many different environments, including enterprise and service provider environments. Each sensor addresses the bandwidth requirements at one of several speeds, from 80 Mbps to gigabits per second.

The Cisco IDS 4215 can monitor up to 80 Mbps of traffic and is suitable for T1/E1 and T3 environments. Additionally, multiple sniffing interfaces are supported on the IDS-4215 which allow the ability to simultaneously protect multiple subnets, thereby delivering five sensors in a single unit.

At 250 Mbps, the Cisco IDS 4235 can be deployed to provide protection in switched environments, on multiple T3 subnets, and with the support of 10/100/1000 interfaces it can also be deployed on partially utilized gigabit links.

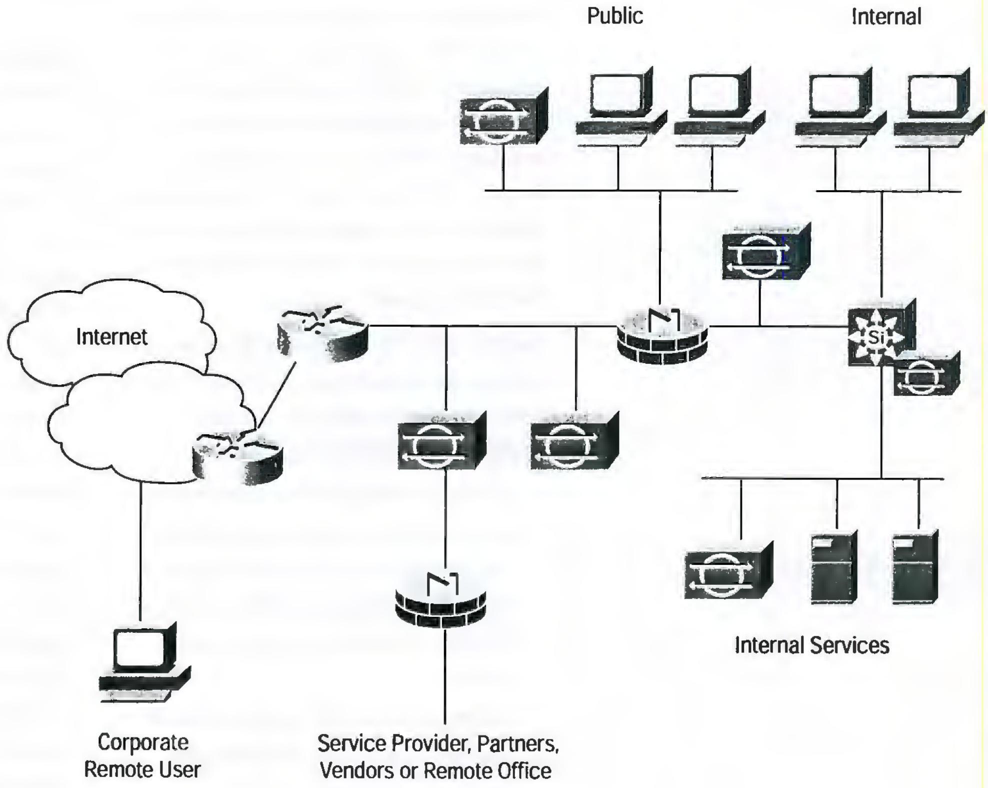
The Cisco IDS 4250 supports a 500 Mbps speed and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets. In addition, the Cisco IDS 4250 provides the flexibility to accommodate a simple hardware upgrade to scale to full line-rate gigabit performance.

At 1 Gbps, the Cisco IDS 4250-XL provides unprecedented performance by providing customized hardware acceleration to protect fully-saturated gigabit links as well as multiple partially-utilized gigabit subnets.

As shown in Figure 1, sensors can be placed on almost any network segment of the enterprise-wide network where security visibility is required.

Please refer to Table 2 for ordering information for the Cisco IDS 4200 Series Sensors.

Figure 1
Deployment Scenarios for the 4200 Series Appliance Sensors



Product Specifications

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Performance	80 Mbps	250 Mbps	500 Mbps	1000 Mbps
Standard monitoring interface	10/100BASE-Tx	10/100/1000BASE-TX	10/100/1000BASE-TX	Dual 1000BASE-SX interface with MTRJ
Standard command and control interface	10/100BASE-Tx	10/100/1000BASE-TX	10/100/1000BASE-TX	10/100/1000BASE-TX
Optional interface	Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	-1000BASE-SX (fiber) -Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	1000BASE-SX (fiber)
Performance upgradable	No	No	Yes	No
Form factor	One rack unit	One rack unit	One rack unit	One rack unit
Advanced protection algorithms				
Stateful pattern recognition	Yes	Yes	Yes	Yes
Protocol parsing	Yes	Yes	Yes	Yes
Heuristic detection	Yes	Yes	Yes	Yes
Anomaly detection	Yes	Yes	Yes	Yes
Attack protection				
Sweeps or floods	Yes	Yes	Yes	Yes
Denial-of-service (DoS) mitigation	Yes	Yes	Yes	Yes
Worms or viruses	Yes	Yes	Yes	Yes
Common gateway interface (CGI) or WWW attacks	Yes	Yes	Yes	Yes
Buffer overflow protection	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Remote-procedure call (RPC) attack detection	Yes	Yes	Yes	Yes
IP fragmentation attacks	Yes	Yes	Yes	Yes
Internet Contro Message Protocol (ICMP) attacks	Yes	Yes	Yes	Yes
Simple Message Transfer Protocol (SMTP), Sendmail, Internet Message Access Protocol (IMAP), or Post Office Protocol (POP) attacks	Yes	Yes	Yes	Yes
File Transfer Protocol (FTP), Secure Shel Protocol (SSH), Telnet, and rlogin attacks	Yes	Yes	Yes	Yes
Domain Name System (DNS) attacks	Yes	Yes	Yes	Yes
TCP hijacks	Yes	Yes	Yes	Yes
Windows or NetBios attacks	Yes	Yes	Yes	Yes
TCP application protection	Yes	Yes	Yes	Yes
BackOrifice attacks	Yes	Yes	Yes	Yes
Network Timing Protocol (NTP) attacks	Yes	Yes	Yes	Yes
Customizable signatures using Signature Micro-Engine technology	Yes	Yes	Yes	Yes
Automated signature updates	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Alarm summarization	Yes	Yes	Yes	Yes
Support for 802.1q traffic	Yes	Yes	Yes	Yes
P2P / file sharing detection techniques	Yes	Yes	Yes	Yes
Secure communication				
IP Security (IPSec) or Secure Sockets Layer (SSL) between sensor and management console	Yes	Yes	Yes	Yes
Encrypted signature packages	Yes	Yes	Yes	Yes
SSH for remote administration	Yes	Yes	Yes	Yes
Serial Control Protocol (SCP) support for secure file transfer	Yes	Yes	Yes	Yes
IDS evasion protection				
IP fragmentation re-assembly	Yes	Yes	Yes	Yes
TCP stream re-assembly	Yes	Yes	Yes	Yes
Unicode deobfuscation	Yes	Yes	Yes	Yes
Active response actions				
Router access-control-list (ACL) modifications	Yes	Yes	Yes	Yes
Firewall policy modifications	Yes	Yes	Yes	Yes
Switch ACL modifications	Yes	Yes	Yes	Yes
Session termination via TCP resets	Yes	Yes	Yes	Yes
IP session logging or session replay	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Active notification actions				
Alarm display	Yes	Yes	Yes	Yes
E-mail alerts	Yes	Yes	Yes	Yes
E-page alerts	Yes	Yes	Yes	Yes
Customizable script execution	Yes	Yes	Yes	Yes
Multiple alarm destinations	Yes	Yes	Yes	Yes
Third-party tool integration	Yes	Yes	Yes	Yes
IDS active update bulletins	Yes	Yes	Yes	Yes
Administration				
Web user interface (Secure Hypertext Transfer Protocol [HTTPS])	Yes	Yes	Yes	Yes
Command-line interface (CLI) (console)	Yes	Yes	Yes	Yes
CLI (Telnet or SSH)	Yes	Yes	Yes	Yes
CiscoWorks VPN Security Management Solution (VMS) support	Yes	Yes	Yes	Yes
High availability				
Redundant power supply	No	Yes	Yes	Yes
Failure detection				
Monitoring link failure detection	Yes	Yes	Yes	Yes
Communications failure detection	Yes	Yes	Yes	Yes
Services failure detection	Yes	Yes	Yes	Yes
Device failure detection	Yes	Yes	Yes	Yes
Dimensions				

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Height	1.7 in. (4.37 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)
Width	16.8 in. (42.72 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)
Depth	11.8 in. (29.97 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)
Weight	11.5 lb (4.11 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)
Rack-mountable	Yes	Yes	Yes	Yes
Power				
Autoswitching	100V to 240V AC	110–220 VAC	110–220 VAC	110–220 VAC
Frequency	50 to 60 Hz	50–60 Hz	50–60 Hz	50–60 Hz
Operating current	1.5A	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V
Operating environment				
Operating temperature	+5°C to +40°C (+41°F to +104°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)
Nonoperating temperature	-25°C to +701/4°C (-13F to +1581/4°F)	–40 to 65°C (–40 to 149°F)	–40 to 65°C (–40 to 149°F)	–40 to 65°C (–40 to 149°F)
Operating relative humidity	5 to 95% (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)
Nonoperating relative humidity	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)
Heat dissipation (most severe case with full power usage)	410 Btu/hr (full power usage (65W))	983 Btu/hr (maximum)	983 Btu/hr (maximum)	983 Btu/hr (maximum)

Note:

- This 80-Mbps performance for the Cisco IDS 4215 is based on the following conditions:
  - 800 new TCP connections per second
  - 800 HTTP transactions per second
  - Average packet size of 445 bytes,
  - Running Cisco IDS 4.0 Sensor Software
- This 250-Mbps performance for the Cisco IDS 4235 is based on the following conditions:
  - 3000 new TCP connections per second
  - 3000 HTTP transactions per second
  - Average packet size of 445 bytes

- Running Cisco IDS 4.0 Sensor Software
- This 500-Mbps performance for the Cisco IDS 4250 is based on the following conditions:
  - 5000 new TCP connections per second
  - 5000 HTTP transactions per second
  - Average packet size of 445 bytes
  - Running Cisco IDS 4.1 Sensor Software
- This 1000-Mbps performance for the Cisco IDS 4250-XL is based on the following conditions:
  - 5000 new TCP connections per second
  - 5000 HTTP transactions per second
  - Average packet size of 595 bytes
  - Running Cisco IDS 4.0 Sensor Software

Regulatory Compliance

- EMC—FCC (CFR 47 Part 15) Class A, CISPR 22 Class A, EN 55022 Class A, EN 55024, EN61000-3-2, EN61000-3-3, VCCI Class A, AS/NZS 3548 Class A, CE marking
- Safety UL 60950, CSA 22.2 No.60950, IEC 60950, EN 60950, AS/NZS 3260, CE marking.

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
IDS-4215-K9	Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100BASE-Tx interfaces with RJ-45 connector), 80-Mbps
IDS-4215-4FE-K9	Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100BASE-Tx interfaces with RJ-45 connector plus 4FE interface card), 80-Mbps
IDS-4235-K9	Cisco IDS 4235 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
IDS-4250-TX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
IDS-4250-SX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 1000BASE-SX with SC connector)
IDS-4250-XL-K9	Cisco IDS 4250-XL Sensor (chassis, software, SSH, hardware accelerator, with dual 1000BASE-SX and MTRJ connectors)
IDS-XL-INT=	Cisco IDS Accelerator Card with dual 1000BASE-SX interfaces and MTRJ connectors
IDS-4250-SX-INT=	1000BASE-SX monitoring interface with SC connector
IDS-4FE-INT=	Spare 4FE (10/100 BaseTx) sniffing interfaces for 4215, 4235, & 4250
IDS-PWR=	Spare power supply for the Cisco IDS 4235 and 4250 sensors
IDS-SCSI=	Spare Small Computer Systems Interface (SCSI) hard disk drive for Cisco IDS 4250 Sensor
IDS-RAIL-2=	Two post rail kits for the Cisco IDS 4235 and 4250 sensor platforms
IDS-RAIL-4=	Four post rail kits for the Cisco IDS 4235 and 4250 sensor platforms

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
CON-SNT-IDS4215XK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4215-K9)
CON-SNTE-IDS4215XK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4215-K9)
CON-SNTP-IDS4215XK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4215-K9)
CON-OS-IDS4215XK	Cisco SMARTnet Onsite support 8 x 5 x NBD (Cisco IDS 4215-K9)
CON-OSE-IDS4215XK	Cisco SMARTnet Onsite support 8 x 5 x 4 (Cisco IDS 4215-K9)
CON-OSP-IDS4215XK	Cisco SMARTnet Onsite support 24 x 7 x 4 (Cisco IDS 4215-K9)
CON-SNT-IDS4215-4FEXK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4215-4FE-K9)
CON-SNTE-IDS4215-4FEXK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4215-4FE-K9)
CON-SNTP-IDS4215-4FEXK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4215-4FE-K9)
CON-OS-IDS4215-4FEXK	Cisco SMARTnet Onsite support 8 x 5 x NBD (Cisco IDS 4215-4FE-K9)
CON-OSE-IDS4215-4FEXK	Cisco SMARTnet Onsite support 8 x 5 x 4 (Cisco IDS 4215-4FE-K9)
CON-OSP-IDS4215-4FEXK	Cisco SMARTnet Onsite support 24 x 7 x 4 (Cisco IDS 4215-4FE-K9)
CON-SNT-IDS4235K9	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4235)
CON-SNTE-IDS4235K9	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4235)
CON-SNTP-IDS4235K9	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4235)
CON-OS-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4235)
CON-OSE-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4235)
CON-OSP-IDS4235K9	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4235)
CON-SNT-IDS4250TK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-SNTE-IDS4250TK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-TX)
CON-SNTP-IDS4250T	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-OS-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-OSE-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x 4 Cisco (IDS 4250-TX)
CON-OSP-IDS4250TK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-SNT-IDS4250SK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-SX)
CON-SNTE-IDS4250SK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-SNTP-IDS4250SK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-OS-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-SX)
CON-OSE-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-OSP-IDS4250SK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-SNT-IDS4250XK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-XL)
CON-SNTE-IDS4250XK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-SNTP-IDS4250XK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-XL)
CON-OS-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-XL)
CON-OSE-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-OSP-IDS4250XK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-XL)

6-225 ✓

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
CON-SNT-IDS4FE	Cisco SMARTnet support 8 x 5 x NBD (IDS-4FE-INT=)
CON-SNTE-IDS4FE	Cisco SMARTnet support 8 x 5 x 4 (IDS-4FE-INT=)
CON-SNTP-IDS4FE	Cisco SMARTnet support 24 x 7 x 4 (IDS-4FE-INT=)
CON-OS-IDS4FE	Cisco SMARTnet onsite support 8 x 5 x NBD (IDS-4FE-INT=)
CON-OSE-IDS4FE	SMARTnet onsite support 8 x 5 x 4 (IDS-4FE-INT=)
CON-OSP-IDS4FE	SMARTnet onsite support 24 x 7 x 4 (IDS-4FE-INT=)
CON-SNT-IDSXL	Cisco SMARTnet support 8 x 5 x NBD (IDS-XL-INT=)
CON-SNTE-IDSXL	Cisco SMARTnet support 8 x 5 x 4 (IDS-XL-INT=)
CON-SNTP-IDSXL	Cisco SMARTnet support 24 x 7 x 4 (IDS-XL-INT=)
CON-OS-IDSXL	Cisco SMARTnet onsite support 8 x 5 x NBD (IDS-XL-INT=)
CON-OSE-IDSXL	SMARTnet onsite support 8 x 5 x 4 (IDS-XL-INT=)
CON-OSP-IDSXL	SMARTnet onsite support 24 x 7 x 4 (IDS-XL-INT=)

Export Considerations

The Cisco IDS 4200 Series sensors are subject to export controls. Refer to the export compliance Web site for guidance at: http://www.cisco.com/wwl/export/crypto/.

For specific export questions, contact export@cisco.com.

Additional Information

For more information about the Cisco Intrusion Protection System, go to: http://www.cisco.com/go/ids

For more information about the CiscoWorks VMS Solutions (IDS management), go to: http://www.cisco.com/go/vms

6 224 1
2

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

RD/LW4599 0503

Apêndice EH

Cisco Intrusion **Detection** System

Q. What is a "network-based" IDS?

A. Two basic types of IDSs are on the market today: host-based and network-based systems. The fundamental difference between them is the source of the activity that they monitor and analyze to detect intrusions. Host-based IDSs monitor activity on a host or end system, while network-based IDSs monitor network traffic. Host-based IDSs are used to protect critical network servers or other individual systems containing sensitive information. Network-based IDSs are used to monitor activity on a specific network segment. Whereas a host-based IDS resides on a workstation and shares CPU with other user applications, a network-based solution is a dedicated platform. Network-based IDSs perform a rule-based or expert system analysis of traffic using parameters set up by the security manager, and the signatures, which flag suspicious or attack activity. The systems analyze network packet headers to make security decisions based on source, destination, and packet type. They also analyze packet data to make decisions based on the actual data being transmitted. These systems scale well for network protection because the number of actual workstations, servers, or user systems on the network is not critical, the amount of traffic is what matters. In addition, sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise. The Cisco® network-based Intrusion Detection System provides network administrators with enhanced security technology and capabilities to secure their networks.

Q. If I already have a firewall, do I really need an IDS?

A. Absolutely. Although an IDS will not replace your firewalls or other security devices for that matter, it serves a very complementary role and addresses certain risks that firewalls cannot. The primary function of the firewall is to control access to services and hosts based on your site security policy. If a service or connection to a specific host is permitted, firewalls typically permit all such traffic, and they do not inspect the content of the permitted traffic. An example is permitting public access to a Web server on a DMZ. All connection requests to the Hypertext Transfer Protocol (HTTP) port on that Web server will be permitted by the firewall, including malicious traffic directed at the HTTP server to exploit a buffer overflow vulnerability. Although most firewalls will not protect against data/content-driven attacks (for example, buffer overflow), IDSs will. Furthermore, firewalls typically will not protect you against attacks originating from inside your network or entering your environment from other ingress points not protected by firewalls (for example, remote access servers). IDSs can be strategically deployed to monitor activity from internal sources and other network ingress points without impacting your network. Deploying an IDS to complement your firewall(s) will significantly enhance your security posture.

Q. Is there a mechanism by which users may contact the IDS Product Team at Cisco?

A. Yes. Users may pose questions, requests, and comments to the following e-mail address:

ids-news@cisco.com

In addition, users have the ability to share experiences with other users and also pose questions to the Cisco IDS Engineering & Product Marketing teams at the IDS Networking Professionals Forum at:

http://forums.cisco.com/eforum/servlet/
NetProf?page=netprof&CommCmd=MB%3FcmdDdisplay_messages26mode3Dnew26location%3D.ee6e1fc

Q. Does anyone offer a managed IDS service using the Cisco IDS?

A. Yes, numerous managed service providers offer a managed IDS service using the Cisco IDS. These managed service providers include AT&T, Counterpane, IBM Emergency Response Services, NetSolve, Riptech, RedSiren, and Ubizen.

Sensors

Q. What are the new features of the Cisco IDS 4.0 Sensor software?

A. The Cisco IDS 4.0 Sensor software delivers a number of new features and enhancements to the network-based IDS portfolio. These features include:

- Re-architecture of communications protocol to enhance the efficiency of message transactions
- Common code base to allow feature parity between the appliance sensor and the switch sensor
- Delivery of a Layer 2 signature engine to mitigate issues such as man in the middle attacks and ARP spoofing in switched environments
- Introduction of an SMB engine to efficiently address attacks related to SMB
- Ability to capture the trigger packet that caused an alarm
- Enhanced shunning capabilities to allow shunning by port address
- Major enhancements to our existing protocol anomaly techniques
- Provision of Analysis Statistics Engine to deliver information of metrics such as bad checksums, bytes processed, data rates Mbps, TCP nodes per sec, and other analysis metrics
- Introduction of a full featured Cisco IOS-like CLI (command-line interface) for unprecedented sensor management over a secure SSH connection
- Capability of capture and display of the VLAN ID of the malicious traffic that was detected
- Enhancements to IP Fragmentation Reassembly
- Higher levels of granularity for the alarm information that is transmitted to the management console
- Support for ntp
- NAT support
- Logical signature groupings to allow global changes across the groupings
- Ability to implement exceptions to filter events to be displayed
- Tunability of IP session logging parameters

6.221
L

Q. What performance numbers (Mbps) are supported by the Cisco IDS Sensors?

A. The Cisco IDS 4215 supports 80 Mbps of performance and can be used to protect T1/E1/T3 environments.

At 250 Mbps, the Cisco IDS 4235 can be deployed to provide protection in switched environments, on multiple T3 subnets, and with the support of 10/100/1000 interfaces, it can also be deployed on partially utilized gigabit links.

The Cisco IDS 4250 supports superior performance at 500 Mbps and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets.

Intrusion protection for fully saturated gigabit links is delivered by the Cisco IDS 4250-XL. Using customized hardware acceleration, the IDS-4250-XL can be used to protect gigabit subnets and multiple partially utilized gigabit links.

The Cisco Catalyst® 6500 Series Intrusion Detection System (IDSM-2) Services Module supports 600 Mbps. This module operates within the Catalyst 6500 Series and provides protection for traffic traversing the switch, which could be traffic from a single subnet or from numerous subnets that are being aggregated through the switch.

The Cisco IDS Network Module provides full-featured Intrusion Protection that is integrated into the Cisco 2600, 3600, and 3700 series routers. Each sensor addresses the bandwidth requirements of different routers up to 10 Mbps in the Cisco 2600XM, and up to 45 Mbps in the Cisco 3700 Series. By integrating IDS and branch office routing, Cisco reduces the complexity of securing WAN links and at the same time reduces operational costs. Additionally, by delivering full-featured intrusion protection to remote offices and branch offices, network administrators can now mitigate threats at these remote locations and effectively isolate them from the corporate network. The Network Module has the capability of inspecting GRE/IPsec encrypted packets that are traversing the router into which it integrates.

Q. How does the IDS sensor work?

A. Sensors monitor the network traffic by directly "tapping" the line (for example, via a shared-media hub) or by receiving copies of the traffic (for example, Switched Port Analyzer [SPAN] port on a switch) using a passive, promiscuous interface (the "monitoring interface"). The sensor analyzes the captured packets and compares them against a rule set of typical intrusion activity (that is, "signatures"). If the captured packets match a defined intrusion pattern in the rule set, the sensor sends an alarm to the management console and automatically responds (if configured to do so). The alarms are sent out a separate management interface so as not to impede continual packet capture by the monitoring interface.

Q. What kind of a performance impact does the sensor impose on the monitored network?

A. None. Sensors operate by "tapping" the network (for example, via a shared-media hub) or off copies of the packets (for example, via a switch SPAN port). The monitoring interfaces on the sensors are passive and do not source packets onto the network (the one exception is TCP reset packets for automatic response).

Q. How do you deploy sensors in a switched environment?

A. With most IDS products on the market today, sensors must be placed on the switch SPAN port to monitor network traffic. Although the SPAN port can provide access to network traffic, it does have certain limitations (for example, limited number of SPAN sessions). The Catalyst 6000 IDS Module was designed specifically to address switched environments by integrating the IDS functionality directly into the switch and taking traffic right off the switch backplane.

Q. What is the Cisco IDS Network Module for the Cisco 2600, 3600, and 3700 series routers?

A. The Cisco IDS Network Module is a network module that is installed in a Cisco 2600, 3600, or 3700 series chassis to provide full-featured intrusion protection services within the router. The Cisco 2600, 3600, and 3700 Series IDS Network Module provides the ability to inspect all traffic traversing the router, to identify unauthorized or malicious activity such as hacker attacks, worms, or denial-of-service attacks, and to terminate this traffic to suppress or contain threats.

Q. How does the Cisco IDS Network Module work?

A. The Cisco 2600, 3600, and 3700 Series IDS Network Module receives copies of packets directly from the router's backplane in a passive or promiscuous mode. The packets are passed through the internal monitoring interface for classification and processing. The Cisco 2600, 3600, and 3700 Series IDS Network Module analyzes the captured packets and compares them against a rule set of typical intrusion activity. If the captured packets match a defined intrusion pattern in the rule set, the IDS Network Module can take one of two actions. It can send a command to the router to either shut down the interface or it can send a TCP reset packet to the sender to stop the TCP session causing the attack.

Q. What is the rated performance of the Cisco 2600, 3600, and 3700 Series IDS Network Module?

A. The Cisco 2600, 3600, and 3700 Series IDS Network Module provides up to 10 Mbps for the 2600XM Series and up to 45 Mbps for the 3700 Series, depending on the platform in which the network module is inserted.

Q. Can the Cisco Network IDS Sensors monitor trunked traffic?

A. Both IDSM and the appliance sensors can monitior 802.1q traffic and, hence, are VLAN aware.

Q. What type of interfaces are supported on the appliance sensors?

A. Copper interfaces are supported on the IDS 4215 and IDS 4235. Both Copper and Fiber interfaces are supported on the IDS 4250 Sensor. The 4250-XL supports dual fiber interfaces with MTRJ connectors.

Q. Does Cisco IDS provide multi-interface support?

A. Yes. Dual sniffing interfaces are supported on the IDS 4250-XL. Up to 5 interfaces are supported on the IDS 4215, 4235, and 4250 Sensor appliances.

A configurable four Fast Ethernet interface card is provided for other models of the Cisco 4200 Series sensors to deliver a total of five sniffing interfaces for each sensor—one onboard sniffing interface plus four Fast Ethernet configurable interfaces.

The Cisco IDSM-2 can be used to monitor traffic from multiple interfaces. The network module for the Cisco access routers can monitor traffic from any of the router interfaces.

Q. Is the user notified when the sniffing interface of a sensor is disconnected?

A. Sensors are equipped with a monitoring interface for data packet capture and a command and control interface for transmitting alarms to the management console and receiving configuration information from the management console. When the sniffing interface is disconnected, an alarm is triggered. This setup provides the user with an alert mechanism when the interface is tampered with and, hence, assures persistent operation.

Q. Does the Cisco IDS Sensor provide an indication of when it is oversubscribed?

A. Yes. The sensor, IDSM, and network module issue an alarm when their respective performance ratings are exceeded.

Q. Where can I find more details on the IDS signature algorithms?

A. For more information on the signature algorithms, please refer to a white paper that may be downloaded at:

http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/idssa_wp.htm

Q. Does Cisco IDS protect against common IDS evasion techniques?

A. Cisco IDS also includes protection from a number of advanced, anti-IDS evasion techniques including:

- IP fragmentation reassembly
- TCP streams reassembly
- Unicode Web deobfuscation

Q. Can the sensor itself be attacked and compromised?

A. A properly configured and installed sensor cannot be compromised. The monitoring interface (connected to the production network) cannot be detected, and packets cannot be directed at it. The interface is in promiscuous mode, and has neither a protocol stack nor an IP address bound to it. It is not susceptible to "antisniff" detection techniques. The separate management interface does have an IP address, but Cisco recommends that a separate, isolated management subnet be used to provide connectivity from the management interface on the sensor to the IDS management console. In addition, only a very limited number of services are available from the management interface, and access controls can be configured to allow only designated management systems to connect to the sensor.

Q. What is Cisco Countermeasures Research Team (C-CRT)?

A. The core of the Cisco IDS solution—the advanced protection capabilities—is developed and maintained by C-CRT. This team of elite security professionals is dedicated to:

- Advancing countermeasures research
- Identifying and responding to new threats
- Distributing proactive signature files and signature micro-engines
- Maintaining our network security database (NSDB)
- Contributing research to the Cisco Security Encyclopedia (CSEC)
- Improving the state of threat mitigation science

The C-CRT is comprised of elite "white hat" personnel. C-CRT's esteemed credentials include:

- *Heritage and tenure*—most joined Cisco through the WheelGroup acquisition.
- *Government clearance*—greater than 65 percent have held Secret and Top Secret Department of Defense security clearances.
- *Military backgrounds*—experience logged from USAF Information Warfare Center, Department of Defense (DOD), Department of Energy (DOE), National Security Agency (NSA), Central Intelligence Agency (CIA), or other notable government organizations.
- *Security experience*—average member of the C-CRT has over six years of computer security experience, allowing Cisco to deliver the most mature, accurate, and industry-proven intrusion protection solutions.

Q. Can I create my own signatures?

A. Because the security objectives for each IDS deployment are unique, Cisco IDS adds granularity to the way in which sensors may be tuned to specifically suit the environment in which they are deployed. Using our innovative TAME (Threat Analysis Micro Engine) policy language, users can create new policies or modify existing policies to meet their unique security objectives. Since the TAME policies are decoupled from the sensing application, changes can be made without affecting sensor performance or reliability.

Q. Is it possible to record and replay the IP session of the source IP address that triggered an IDS alarm?

A. IP session logging provides extensive logging that is important for system troubleshooting as well as for reconstructing system events before and after attacks. Cisco IDS augments this capability by converting these logs to a standard TCP dump format that allows them to be viewed and replayed using public domain utilities, such as Ethereal and TCPReplay.

Q. Can the sensor detect attacks if the traffic is encrypted, for example IPsecurity (IPsec) or Secure Sockets Layer (SSL)?

A. The Cisco IDS Sensor analyzes both packet header information (context data) and packet data information (content data) to determine if suspicious activity is occurring. Encryption algorithms encrypt the data portion of the packet for confidentiality. Because it can process only what it can "see," the Sensor cannot detect attacks that require inspection of the payload or data fields within a packet. It will, however, still alarm and respond to attacks, which are detected from the unencrypted packet header information. All network-based IDSs suffer this problem. Therefore, in networks carrying encrypted traffic, Sensor placement is critical. To take advantage of their full intrusion-detection capability, the Cisco IDS Sensors should be installed where the traffic has already been decrypted. Otherwise, the Sensor can be placed on an encrypted segment and will detect all but the packet data or payload-based attacks.

Q. What techniques does Cisco use for mitigating threats?

A. Several techniques provide comprehensive protection against the latest cyber threats, including simple pattern matching, stateful pattern matching, protocol anomaly detection, heuristic-based detection, and anomaly detection.

Q. Does Cisco IDS deliver Peer to Peer signatures?

A. Yes. Cisco IDS delivers protection against file-sharing threats with support for advanced P2P attack mitigation techniques.

Q. How are the Cisco IDS signatures updated?

A. Cisco posts signature updates on Cisco Connection Online (CCO) approximately every 14 days. Cisco IDS provides a facility to automatically distribute new signature files and application upgrades to sensors without operator involvement. Utilizing a secure staging technique, new signature files are placed on a central server and passed to the sensor at scheduled intervals. After verifying the integrity of the package, the sensor automatically installs the update. This new capability significantly streamlines the process of regularly updating remote sensors, thereby lowering the recurring operational costs associated with this task. Additionally, users can subscribe to Cisco Active Update notification services to stay informed about breaking vulnerability news and posted countermeasures at:

http://www.cisco.com/warp/public/779/largeent/issues/security/idsnws/archive.html

Users may refer to the following site for a chronological listing of the Cisco IDS Active Update Notification Bulletins:

http://www.cisco.com/warp/public/779/largeent/issues/security/idsnws/archive.html

Q. How do the Cisco IDS Sensors and management consoles communicate with each other?

A. Communication between the Cisco IDS 4.0 Sensors and management consoles is provided by a secure (SSL) XML based messaging format. All alarm transmissions from the sensor to the management console are acknowledged.

If connectivity from the sensor to the management console is disrupted, the sensor will continue to monitor the network, and will queue alarms and retransmit until successful.

Q. How much additional network traffic does the Cisco IDS generate?

A. Because each alarm and acknowledgment is contained in a single UDP packet, there is negligible impact on network traffic.

Q. Is there a site that lists all the supported Cisco IDS signatures?

A. Yes. Users may access the latest Cisco IDS signatures at the Cisco Secure Encyclopedia site at:

http://www.cisco.com/pcgi-bin/front.x/csec/idsHome.pl

Q. Does Cisco support a centralized site that contains a compiled listing of the latest vulnerabilities?

A. Yes. Cisco's Security Encyclopedia is a one-of-a-kind clearinghouse of security and vulnerability information. Unlike other security databases that simply consolidate vulnerability information published on a number of public-source Web sites, the CSEC contains statistics on the vulnerabilities by industry or by sector. These statistics are compiled from over 400 actual Security Posture Assessments (SPA) performed by the Cisco Security Consulting team. CSEC is developed and maintained by the elite C-CRT. You may visit the CSEC site at:

http://www.cisco.com/go/csec

Q. Where can I download the latest IDS software?

A. Both current and archived IDS Sensor software can be downloaded at the Software Center on CCO (CCO login required):

http://www.cisco.com/public/sw-center/ciscosecure/ids/crypto/

Q. Where can I access documentation on the Cisco IDS Sensor Software?

A. Documentation for sensor software updates are available at:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm

Threat Response Technology

Q. Is Threat Response an event correlator?

A. Threat Response is not an event correlator. Event correlation involves analyzing data from NIDS sensor, firewalls, routers, and other sources. Instead of correlating this type of data, Threat Response investigates the actual target of an attack. This is the same process an expert network security specialist would use, and is the best way to determine if a system has been compromised.

Q. Does Threat Response conduct network vulnerability scans?

A. No, Threat Response does not conduct enterprise wide scans of your environment, nor does Threat Response inventory your network. The designers of Threat Response have been network administrators for large mission-critical enterprises such as the U.S. Pentagon and know that downtime is unacceptable. Because of this, Threat Response conducts a low-impact investigation of targeted systems only when needed. Threat Response is able to work in dynamic network environments (including DHCP and wireless) without the need to run regular vulnerability scans that can disrupt your enterprise.

Q. Does Threat Response require deployment of software across the enterprise?

A. No, Threat Response does not require the deployment of software across the enterprise. Threat Response accesses these systems in the same way a security network administrator would—with read access privileges.

Q. How does Threat Response stay up to date with the latest attacks?

A. Cisco releases updates to keep the Threat Response IDS signature database up to date with the IDS vendors, as well as corresponding forensic signature updates to investigate IDS events. When an update is available, the administrator will be notified via the Threat Response GUI and can use the integrated auto-update feature to keep the product current.

Q. What does Threat Response do once real attacks are identified?

A. Threat Response will provide the user with detailed information on how the event was investigated, as well as any forensic data gathered showing details on the actual attack. This information can then be used by an administrator to quickly remediate an intrusion.

Q. What type of systems can Threat Response investigate?

A. Threat Response can conduct a full active investigation of systems running Windows-based operating systems. For systems running Linux, Solaris, and other forms of UNIX, Threat Response will perform passive checks as a first line of investigation. Based on this initial analysis, Threat Response can eliminate many alarms that are not targeted to those specific platform types.

Q. How do I get Threat Response technology?

A. Threat Response technology is currently available as a full featured, 90-day free trial software solution. The trial version ships with every Cisco IDS sensor. Once the trial has expired, customers have the choice of:

- switching to a reduced capabilities free version (only conducts basic level investigation of the targeted system)
- purchasing the full featured version, which will be offered as part of a VMS bundle

Management

Q. What management console options are available for the Cisco IDS?

A. See Table 1 and Table 2.

Table 1 Event Management

	IEV	IEV with CTR Technology	VMS SecMon	VMS SecMon with CTR Technology
Deployment method	Dedicated system required	Dedicated system required	Dedicated system required	Dedicated system required
GUI type	Java desktop application	Browser-based GUI	Browser-based GUI	Browser-based GUI
# sensors	5	5	Unlimited	Unlimited
Event types	IDS	IDS	IDS, Firewall, Router	IDS, Firewall, Router

Table 2 Device Management

	IDM	CLI	VMS Management Center
Deployment method	Integrated on sensor	Integrated on sensor	Dedicated system required
GUI type	Browser-based GUI	Browser-based GUI	Browser-based GUI
# sensors	Unlimited, by sensor	Unlimited, by sensor	Unlimited, by sensor groups
Event types	IDS	IDS	IDS, Firewall, Router

IEV = Cisco IDS Event Viewer, included free of charge with IDS sensor
VMS SecMon = CiscoWorks Monitoring Center for IDS, part of the CiscoWorks VMS bundle
IDM = IDS Device Manager, included free of charge with the IDS sensor
CLI = Command-line interface, included free of charge with the IDS sensor
VMS Mgmt Center = CiscoWorks Management Center for IDS, part of the CiscoWorks VMS bundle

For More Information

More information on Cisco's VMS solutions can be found at:

http://www.cisco.com/go/vms

In addition, augmentation to the alarm viewing, analysis, and reporting capabilities of the Cisco IDS Management solution are provided through third-party applications that are available from Cisco Security Associates partners.

For more details see:

http://www.cisco.com/warp/public/778/security/sap/management.html

Q. Are Cisco IDS communications encrypted?

A. IPsec functionality is included on the appliance Sensors to allow customers to encrypt traffic to management consoles with IPsec capabilities.

Q. If I lose connectivity to a remote sensor, can I tell from the management console?

A. The Cisco IDS management consoles monitor the health of a Sensor via a continuous heartbeat. If communications with the Sensor are lost for more than one minute (by default), a visual indicator is displayed on the management console, indicating a communications failure with the Sensor. If it is determined that a sensor has failed, it can be quickly replaced with another sensor and the configuration, stored on the management console, and can be quickly pushed to the new sensor.

Q. How many sensors can one Cisco IDS Management console manage?

A. Although the technical limit is very large (greater than 1000), Cisco typically recommends a ratio of 20 to 25 sensors per management console for practical reasons. With ratios greater than this, operators can be easily overwhelmed with the volume of information that they may be required to analyze, thereby diminishing the overall effectiveness of the IDS. For deployments larger than 25 sensors, multiple management consoles can be installed to scale the number of sensors.

Q. Can I have multiple Cisco IDS management consoles?

A. The Cisco IDS architecture supports the deployment of multiple management platforms. Sensors can send alarms to multiple management consoles simultaneously, and management consoles can forward alarms to other management consoles, allowing customers to build large, hierarchical management infrastructures.

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

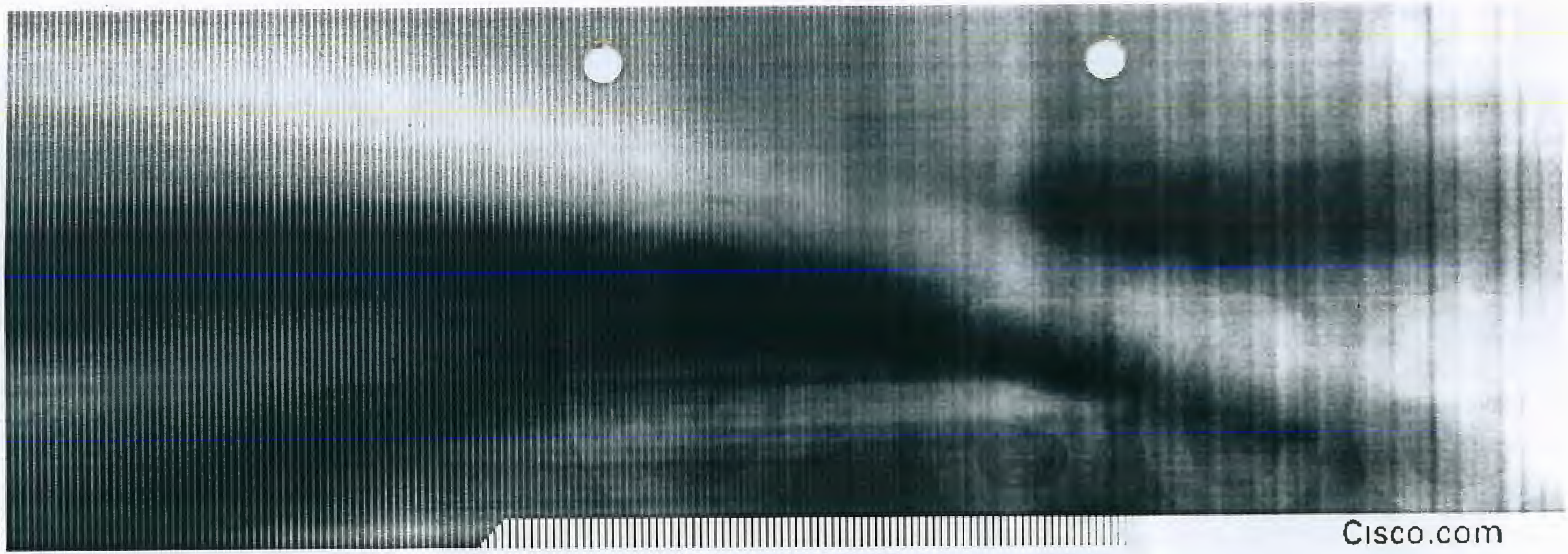
Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice EI

CISCO SYSTEMS



Cisco.com

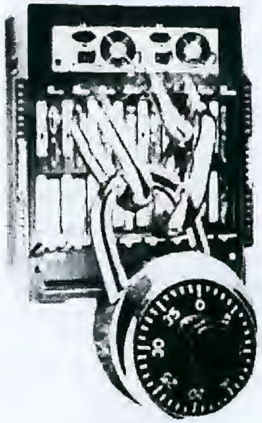
Complete Intrusion Protection

Cisco Security Solutions

Security and Business Resilience

Cisco.com

Secure Connectivity



VPN

Perimeter Security

Firewalls

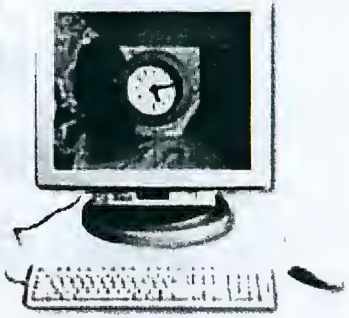
Intrusion Protection

Intrusion Detection Scanning

Identity

Authentication

Security Management



Policy

Appliance Overlay Solutions

Network Integrated Solutions

Management Applications

Server-Based Services Software

Cisco IDS Accomplishments

Innovation – Leadership - Expertise

- 1996: First commercial network IDS
- 1998: Acquisition of WheelGroup
- 1999: Integration into Cisco IOS software
- 2000: Migration into Catalyst switch hardware
- 2001: Extensions of IDS appliance line and software
- 2002: Introduction of Gigabit sensing, embedded management, new Enterprise-class management and monitoring, intent to acquire Psionic
- 2003: Hardware-accelerated Gigabit sensing, converged code, false-positive reduction, in-line IDS, extended network integration

Efficient Intrusion Protection
Value Proposition

Efficient Intrusion Protection customers can deploy today:

- Accurate Threat Detection
- Intelligent Threat Investigation
- Ease of Management
- Flexible Deployments Options

6209
7

Cisco's Unique Approach

Cisco.com

- Delivering dedicated and network integration devices – horizontal integration
- Increasing accuracy and reducing false-positives with combination of multi-mode threat detection and newly acquired threat response investigation
- Minimizing Total Cost of Ownership with hardware-integrated solutions and easy-to-use, scalable management and monitoring applications
- Leveraging seven years of leadership and innovation in IDS industry delivering accurate, reliable, and proven solutions. Team of security experts.

Pervasive Protection

IDS Everywhere

Cisco.com

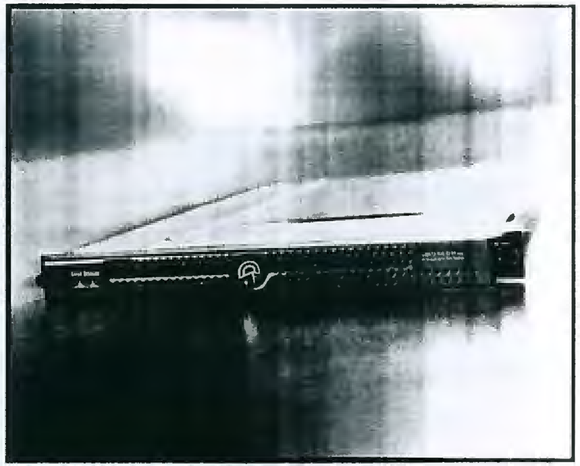
		Solution Breadth				
Network Sensor		4210	4235	4250	4250-XL	
Switch Sensor		IDSM-1	IDSM-2			
Host Sensor		Standard Sensor	Web Sensor			
Router Sensor		1700	2600	3600	7200	
Firewall Sensor		501	506E	515E	525	535
Mgmt		Secure Command Line	Web UI Embedded Mgr	Enterprise Mgmt VMS		

2

Gigabit Sensor Appliance - IDS-4250-XL

Performance-optimized, turn-key appliance

- 1000 Mbps performance
- NPU-based accelerator card
- Multiple sniffing interface support
- Integrated, web-based UI
- 1 RU form factor
- Optional redundant power

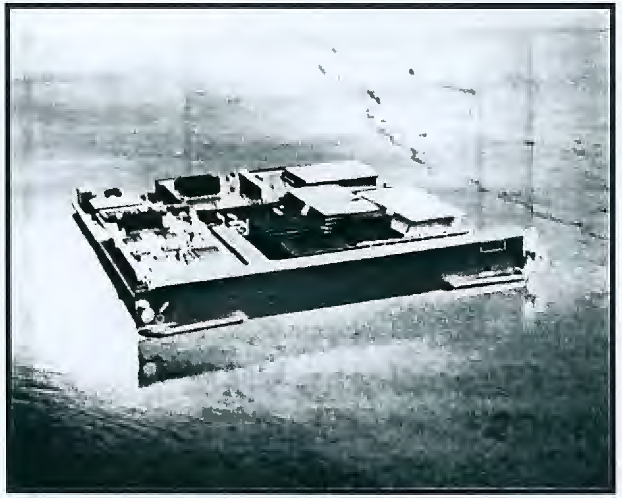


IDS 4250-XL
Performance: 1000 Mbps
Price: $40,000
Availability: Feb. '03

2nd Gen. Catalyst 6500 Module - IDSM-2

Network integrated security services module

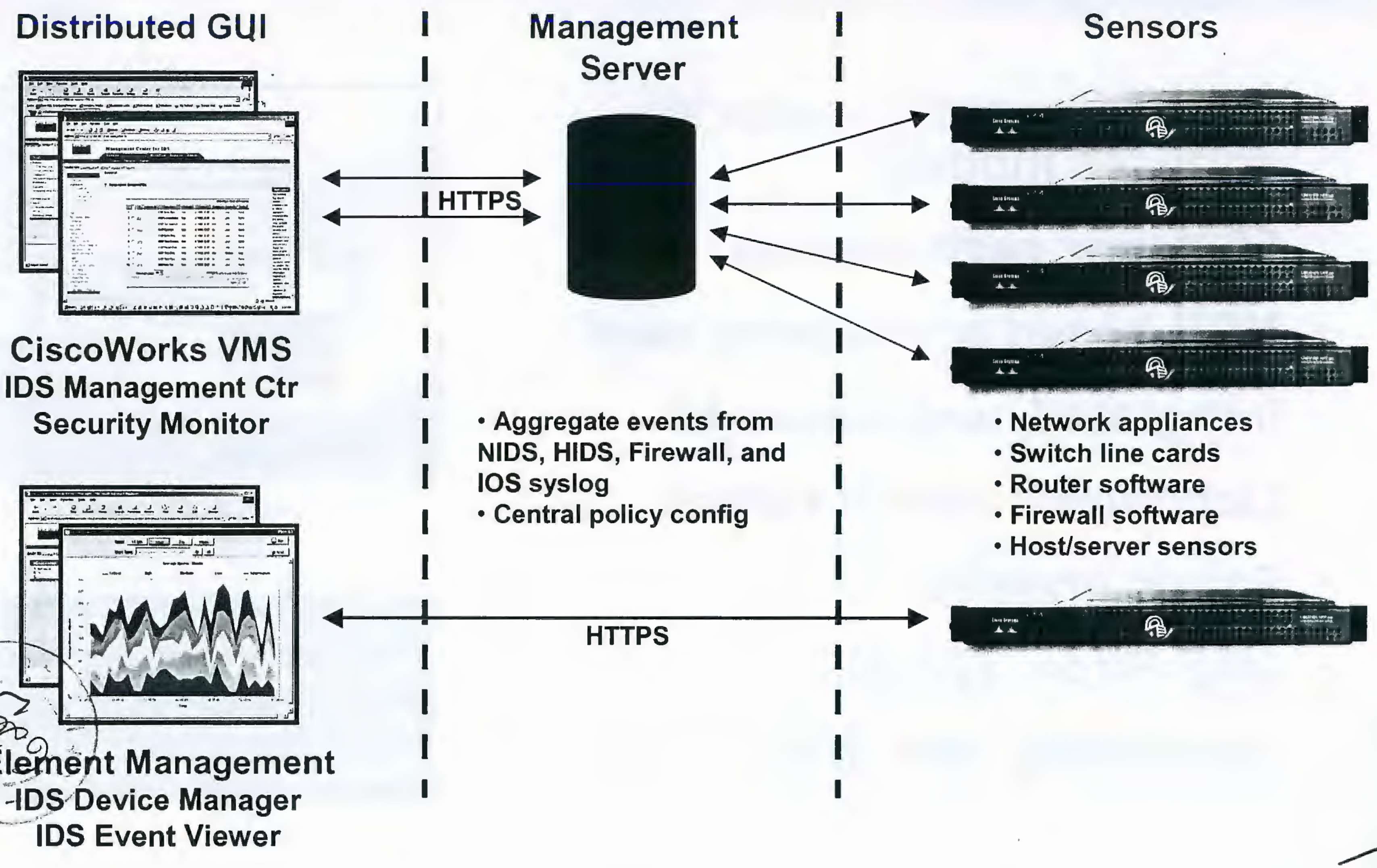
- 600Mbps performance
- NPU-based accelerator card
- Integrated, web-based UI
- Occupies 1 slot in switch
- Fabric enabled
- *NTE Price: $29,995*
- *Availability: Mar 2003*



IDSM-2
Performance: 600 Mbps
NTE Price: $29,995
Availability: Feb. '03

2

Multi-Tiered Architecture



Distributed GUI

CiscoWorks VMS
IDS Management Ctr
Security Monitor

Element Management
IDS Device Manager
IDS Event Viewer

Management Server

- Aggregate events from NIDS, HIDS, Firewall, and IOS syslog
- Central policy config

Sensors

- Network appliances
- Switch line cards
- Router software
- Firewall software
- Host/server sensors

Robust Sensing Protection

- Accurate Detection

  Leverage Multi-Mode Threat Detection

  Simple pattern matching, stateful pattern matching, protocol decoding, and heuristics analysis

  Unique Adaptive Scanning to validate events

- Reliable System

  Hardware-based, single vendor

- Active Response

  In-line: Drop packet or reset connection

  Passive: Reset connection or modify router/firewall

- Flexible Design

  T.A.M.E. signature language

  Customizable thresholds

  Broad delivery options – appliance, modules, line cards, agents

Scalable Configuration Management

- Enterprise Scale

  Manage 100s of devices

  Control IDS, FW, and VPN

- Flexible Device Grouping

  Group devices by function, by location, by configuration to perform mass configuration

  Deploy global settings quickly

- Roles-based Access Control

  Control administrative access to ensure authorization

- Secure Communications

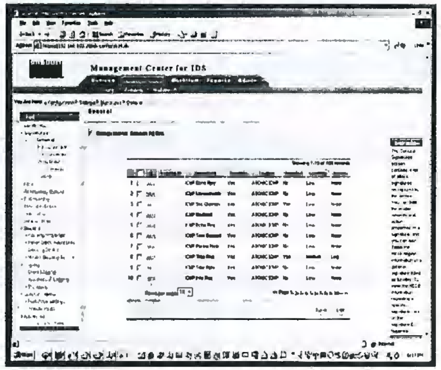
- Tiered Approval Model (optional)

  Separate configuration definition and deployment (maker-checker model)

- Granular Device Control

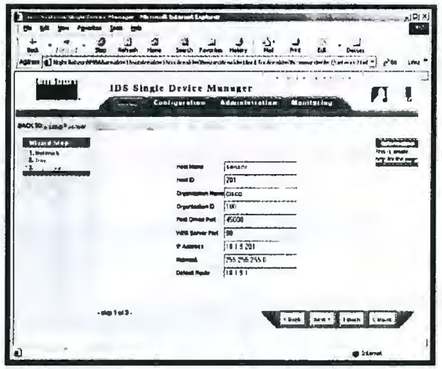
  Device embedded UI for detailed configuration control

Enterprise Management



Management Center for IDS

Device Management



IDS Single Device Manager

Host ID 201

Organization Name cisco

Organization ID 100

Post Office Port 45000

WEB Server Port 80

IP Address 10.1.9.201

Netmask 255.255.255.0

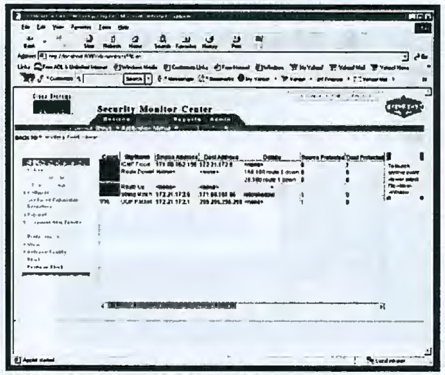
Default Route 10.1.9.1

Threat Monitoring and Investigation

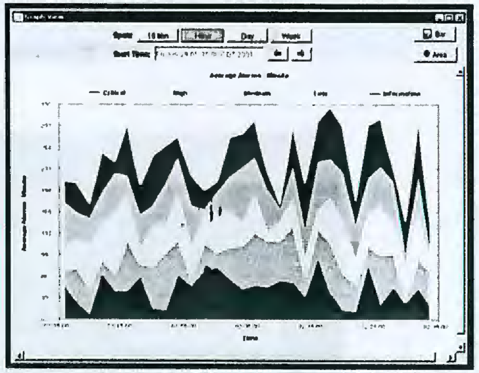
Cisco.com

- Unified Security Monitoring
  - IDS Events (NIDS + HIDS)
  - PIX Syslog
  - IOS Security Syslog
- Real-Time Threat Dashboard
  - Interface Quick Look for threat identification and suppression
- Event Correlation
  - Corroborating events to increase accuracy and minimize false-alarms
  - User defined rules for customization
- Flexible Notification
  - Paging and email to focus operator's attention to most critical alerts
- On-Demand and Scheduled Reporting
  - Flexible reporting by top incidents, by IP address, by time, by signature, by event, etc.

Threat Analysis Console



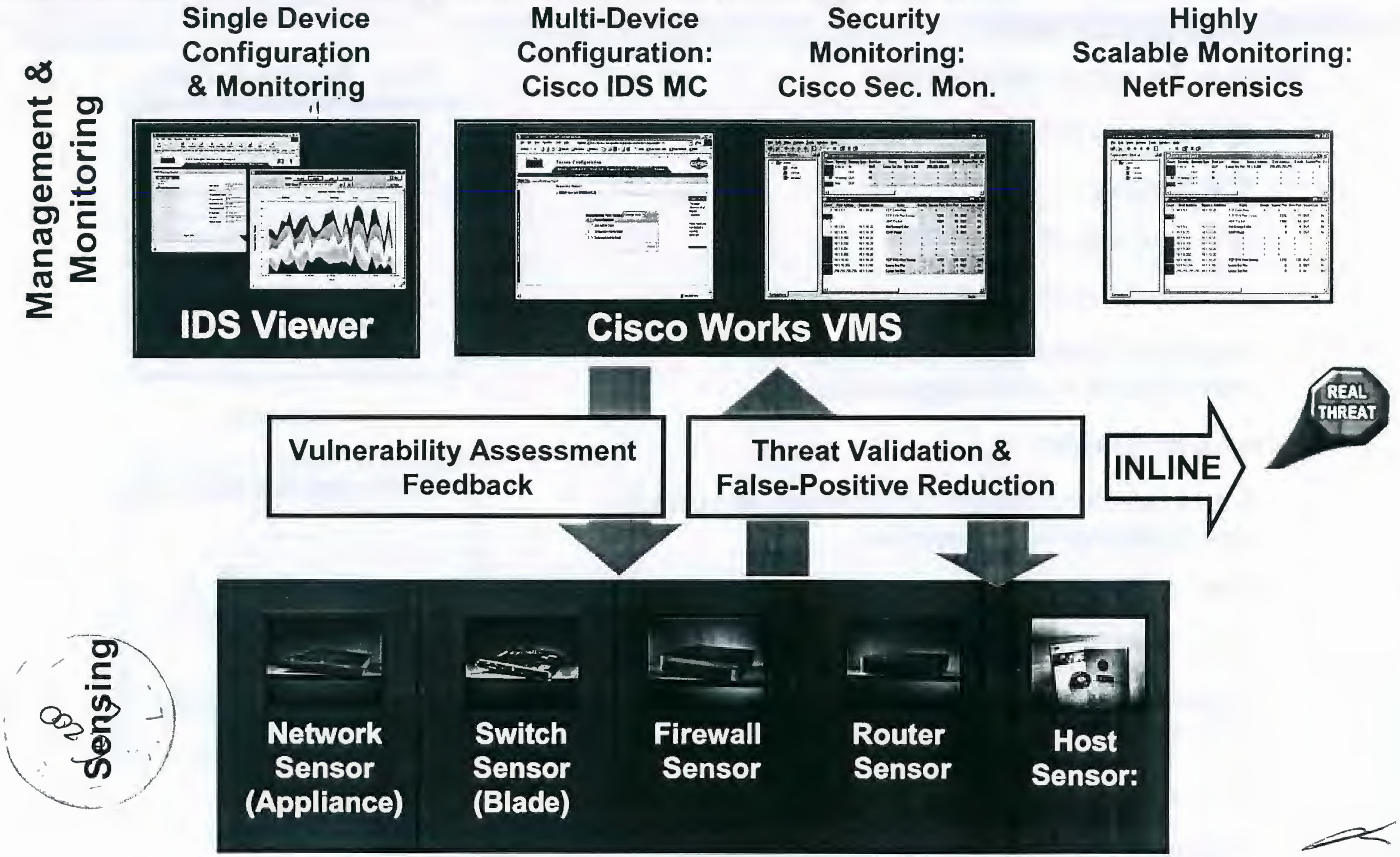
Real-Time Threat Dashboard



Cisco IDS Strategy

Evolution to True Protection

Cisco.com



Management & Monitoring

Single Device Configuration & Monitoring

Multi-Device Configuration: Cisco IDS MC

Security Monitoring: Cisco Sec. Mon.

Highly Scalable Monitoring: NetForensics

IDS Viewer

Cisco Works VMS

Vulnerability Assessment Feedback

Threat Validation & False-Positive Reduction

INLINE

REAL THREAT

Sensing

002

Network Sensor (Appliance)

Switch Sensor (Blade)

Firewall Sensor

Router Sensor

Host Sensor:

IDS Version 4.0

Cisco.com

- Convergence of IDS code bases

  Develop once, populate many

  Feature parity

  Consistent user experience

- Entry into “true” Gigabit IDS market

  Custom HW acceleration card (Intel IXP 1200)

  500 Mb appliances & IDSMs field upgradeable

- False-Positive Reduction

  Release new Cisco Threat Response product

  Extend our protocol analysis

- Remote Data Exchange Protocol (RDEP)

  XML-based configuration and event generation

  Pull vs. push method for event collection & analysis

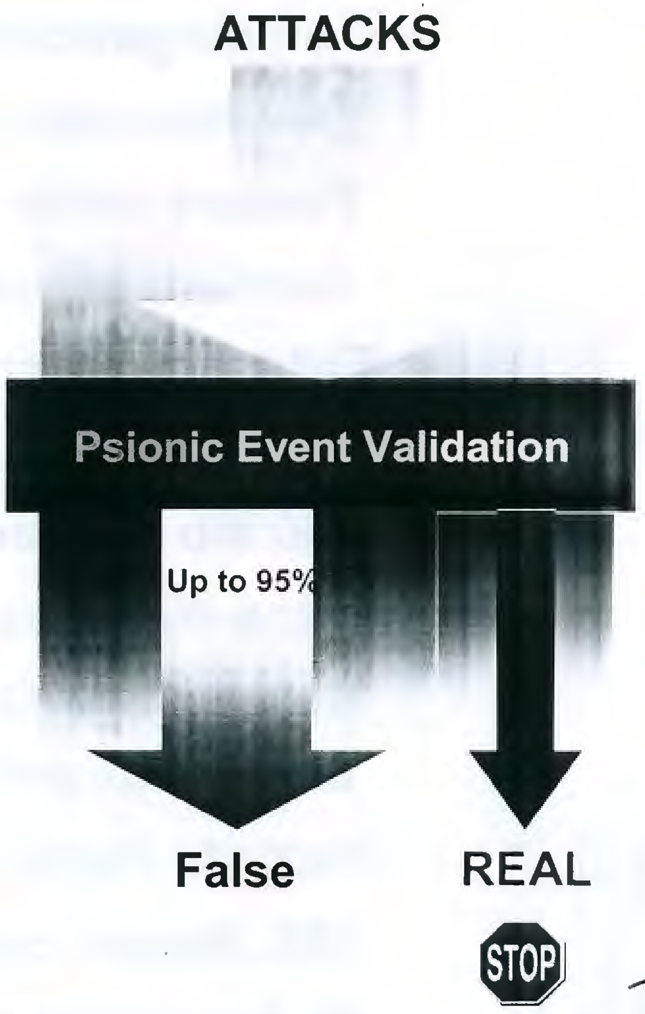
Advantages Cisco Threat Response

- Lowers cost of ownership by reducing false alarms up to 95%
- Uses patented adaptive scan techniques to
  - Validate IDS events
  - Escalate real attacks
  - Aid in remediation of costly intrusions
- Benefits

  Minimizes insignificant events against invulnerable systems

  Increases productivity of users enhancing accuracy

  Decreases time and manpower to deploy and manage IDS systems



6-198

More Than Just Products

- World-wide Training
  - Cisco IDS Course (NIDS & HIDS)
- Certification
  - Cisco Security Specialization
  - CCIE - Security
- Support
  - Award-winning, world-wide, 24x7 support
  - Four-hour replacement equipment available
  - Cisco Countermeasure Research Team (C-CRT)
- User Community
  - IDS Forum via Cisco Network Professional
  - IDS Newsletter & Active Update notification

Cisco Systems

Empowering the Internet Generation℠

Cisco will Acquire Psionic Software, Inc.

- Psionic develops security software (ClearResponse)

  Increases efficiency and reduces complexity and total cost of ownership associated with IDS systems by reducing false alarms up to 95%

- Cisco will integrate Psionic's technology with our broad IDS product family

  Provides high-performance security attack identification and suppression across a range of network environments

  Arms enterprise customers with a more comprehensive class of Intrusion Protection technology while minimizing typical IDS operational costs

2

Cisco IDS Ecosystem – AVVID Partners

Cisco.com

Services Partners

BERBEE

@stake Where Security & Business Intersect

Counterpane Internet Security

ubizen

KPMG

GUARDENT

riptech

NCR Transforming Transactions into Relationships

AT&T

TRUSECURE CORPORATION

EXODUS

NETSOLVE

ThruPoint

IBM

PREDICTIVE SYSTEMS

Product Partners

ARBOR NETWORKS

OpenSystems.com

e-Security

SOLSOFT

Telemate.Net SOFTWARE

Tivoli

NIKSUN

entercept SECURITY TECHNOLOGIES

PENTASAFE securing the digital economy

hp

6·194

2

Apêndice EJ

CiscoWorks **VPN/Security Management** Solution Version 2.2

CiscoWorks VPN/Security Management Solution (VMS) is the flagship integrated security management solution from Cisco, and is an integral part of the SAFE Blueprint from Cisco for network security. CiscoWorks VMS protects the productivity and reduces operating costs for enterprises, by combining Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network and host-based intrusion detection systems (IDS). CiscoWorks VMS delivers the industry's first robust and scalable foundation and feature set that addresses the needs of small and large-scale VPN and security deployments.

Today's business challenges and resulting security deployments require more scalability than merely supporting a large number of devices. Many customers have limited staffing, yet are asked to manage a myriad of security devices. These customers must manage the security and network infrastructure; frequently update many remote devices; implement change control and auditing when multiple organizations are involved in defining and deploying policies; enhance security without adding more headcount; or roll out remote access VPNs to all employees and monitor the VPN service.

CiscoWorks VMS enables customers to deploy security infrastructures from a small to large environment, using the following multifaceted scalability features:

- Complete SAFE Blueprint Coverage

  To completely manage a SAFE environment, a network management solution must manage SAFE infrastructure components, support features based upon an appliance or Cisco IOS® Software, and support a range of management functions. CiscoWorks VMS is uniquely able to scale across SAFE Blueprint components, including firewalls, VPNs, and network- and host-based IDSs. CiscoWorks VMS also takes advantage of Cisco Secure Access Control Server (ACS) by using a common ACS logon. CiscoWorks VMS can manage a feature set through an appliance, for example, the Cisco PIX® Firewall, or through the Cisco IOS Software. Scalable management also involves more than configuring devices. CiscoWorks VMS provides the complete range of management with features to configure, monitor, and troubleshoot the network.

- Scalable Foundation

  CiscoWorks VMS implements a foundation with a consistent user experience, which makes it easier to scale management to many devices. CiscoWorks VMS provides users with a consistent GUI, workflow, ACS logon, roles definition, platforms, database

engine, installation, and more. An industry-leading feature of this foundation is the Auto Update feature, which allows numerous devices to be updated easily and quickly. Auto Update enables devices, even remote and dynamically addressed devices, to periodically "call home" to an update server and "pull" the most current security configurations or Cisco PIX operating system. Auto Update is required to effectively scale remote office firewall deployments across intermittent links or dynamic addresses. Prior policy updating methods relied on a "push" model. Although this model works for known devices, it does not work for remote devices with unknown addresses or devices that are not always active. Without Auto Update a more manual process is required to update each remote device. The Auto Update feature provides a dramatic scalability improvement for organizations that want to deploy devices with many remote and local locations. In addition to easier and faster policy updates, Auto Update also provides consistent policy deployments.

- Enterprise Operational Integration

  CiscoWorks VMS enables organizations to easily integrate management into their operations. One operational need is to replicate policies to multiple locations. The Smart Rules hierarchy addresses this need, by enabling administrators to define device groups and implement policy inheritance. For example, an administrator can define a device group for the New York sales office and deploy that same policy to all other sales offices quickly and consistently. The Command and Control Workflow feature provides change control and auditing, and is particularly important for customers who have separate groups for network and security operations. The solution includes processes for generating, approving, and deploying configurations. This can help security operations to define and approve new policies. Network operations can later deploy the new policies during their regular maintenance window. An audit of the changes can be maintained.

- Centralized Role-Based Access Control (RBAC)

  Role-based access control enables organizations to scale access privileges. CiscoWorks VMS conveniently uses a common ACS logon for users, administrators, devices, and applications. CiscoWorks VMS enables different groups to have different access rights across different devices and applications.

- Integrated Infrastructure Management

  Scalability requires that multiple components be managed, not just firewalls, but also VPNs, network- and host-based IDSs, routers, and switches. CiscoWorks VMS not only manages the security infrastructure, but also manages the network infrastructure. Customers benefit from being able to manage these components from one solution. Integrated monitoring is also required to see the larger picture. CiscoWorks VMS provides integrated monitoring of Cisco PIX and Cisco IOS syslogs, and events from network and host-based IDSs, along with event correlation.

CiscoWorks VMS Functions

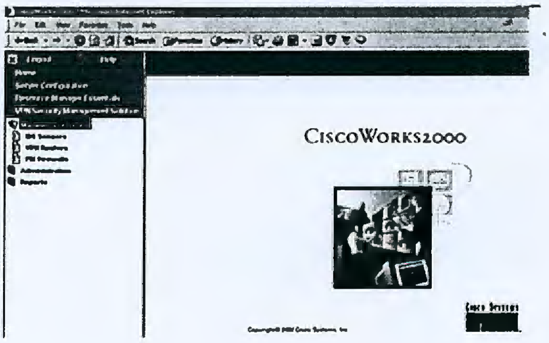
CiscoWorks VMS is launched from the CiscoWorks dashboard and is organized into several functional areas:

- Firewall management
- Auto Update Server
- IDS management, network and host-based
- VPN router management
- Security monitoring
- VPN monitoring
- Operational management

These functional areas supply multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control.

Figure 1 shows CiscoWorks VMS displayed as a "drawer" in the CiscoWorks dashboard.

Figure 1


File Edit View Favorites Tools Help
Logout
Help
Home
Server Configuration
Resource Manager Essentials
VPN Security Management Solution
Administration
Reports
CiscoWorks2000
Cisco Systems

Firewall Management

CiscoWorks VMS enables the large-scale deployment of Cisco PIX firewalls, by providing the following features:

- Smart Rules hierarchy and inheritance
- User-defined device and customer groups including nesting
- Global role-based access with administrative privileges per device and customer groups with other CiscoWorks products and Cisco Secure ACS
- Mandatory and default device settings inheritance
- Workflow deployment to device, directory, or Auto Update Server
- Look and feel of Cisco PIX Device Manager but with scalability to thousands of PIX firewalls
- Integration with other CiscoWorks network management software
- Complete SAFE Blueprint coverage for centralized management of Cisco PIX firewalls, including access control, VPN, IDS, and authentication, authorization, and accounting (AAA)

Smart Rules is an innovative feature that allows common information including access rules and settings to be inherited for all firewalls in a device or customer group. Smart Rules allows a user to define common rules once, which results in reduced configuration time, fewer administrative errors, and higher device scalability. Using Smart Rules, a user can configure a common rule such as allowing all HTTP traffic once and can apply this rule globally to all firewalls. Smart Rules can also be defined on a device or customer group basis. For specific information on the firewall management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3992/index.html

Auto Update Server for Firewall Management

CiscoWorks VMS introduces the industry's first firewall Auto Update Server that allows users to implement a "pull" model for security and Cisco PIX operating system management. Auto Update Server permits remote firewall networks with unprecedented scalability. The Auto Update Server allows Cisco PIX firewalls to both periodically and automatically contact the update server for any security configuration, Cisco PIX Operating System, and PIX Device Manager (PDM) updates. The Auto Update Server supports the following features:

- Security management of remote Cisco PIX firewalls that use Dynamic Host Control Protocol (DHCP)
- Automated Cisco PIX OS distribution to groups of Cisco PIX firewalls
- Automated Cisco PDM updates to remote firewalls
- Configuration verification at periodic intervals
- Automated replacement of inaccurate or tampered configurations
- New firewalls configured at "boot time"

The Auto Update Server is an indispensable component of any large-scale remote Cisco PIX firewall deployment. Auto Update Server is an easy-to-use solution to automatically update all remote or local firewalls with new operating system releases. Cisco is the industry's first vendor to provide this pull model of security policy and operating system management. For specific information on the Auto Update Server component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3993/index.html

Network-Based IDS Management

Administrators can use CiscoWorks VMS to configure network and switch IDS sensors. Many sensors can be quickly configured using group profiles. Additionally, a more powerful signature management feature is included to increase the accuracy and specificity of detection. Some prominent features are:

- Easy-to-use Web-based interface
- Wizards that lead users through common management tasks
- Access to the Network Security Database (NSDB), which provides meaningful information about alarms for users without IDS security expertise
- Ability to define a hierarchy of sensors containing groups and subgroups, and the ability to configure multiple sensors concurrently using group profiles
- Support for several hundred sensor deployments from each console
- Use of a robust relational database to store a high volume of data

For specific information on the network-based IDS management functionality of VMS, refer to:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

Host-Based IDS Management

CiscoWorks VMS provides threat protection for server and desktop computing systems, also known as "endpoints." VMS goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications. Because CiscoWorks VMS analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs. Features of host-based IDS management include:

- Aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent.
- Provides preventive protection against entire classes of attacks including port scans, buffer overflows, Trojan horses, malformed packets, and e-mail worms.
- Offers "zero update" prevention for known and unknown attacks

- Provides industry-leading protection for UNIX and Windows servers and Windows desktops allowing customers to patch systems on their own schedules.
- Open and extensible architecture offers the capability to define and enforce security according to corporate policy.
- Scalable to thousands of agents per manager to support large enterprise deployments.

For specific information on the host-based IDS management functionality of VMS, refer to: the Management Center for Cisco Security Agents Datasheet.

VPN Router Management

CiscoWorks VMS includes functions for the setup and maintenance of large deployments of VPN connections and provides users with a point-and-click interface for setting up and deploying connections. This application is intended for scalable configuration of site-to-site VPN connections in a hub-and-spoke topology for centralized, multidevice configuration and deployment of Internet Key Exchange (IKE) and IP Security (IPsec) tunneling policies on VPN routers.

Major features include:

- Wizard-based interface for the creation of IKE and VPN tunneling policies.
- Hierarchical inheritance and Smart Rules hierarchy to reflect the organizational and common setup of devices and simplified device management
- IKE-KA (IKE Keepalive) or generic routing encapsulation (GRE) with Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) for failover routing scenarios.
- Centralized role-based access control model allows for centralized management of users and accounts.

For specific information on the VPN router management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3994/index.html

Security Monitoring

CiscoWorks VMS provides integrated monitoring to reduce the number of security monitoring consoles, reduce the number of events to monitor, and provide a broader view of security status.

- Integrated monitoring is used to capture, store, view, correlate, and report on events from many of the devices in the SAFE Blueprint such as Cisco network IDSs, switch IDSs, host IDSs, firewalls, and routers.
- Event correlation is used to identify attacks that are not easily recognizable from a single event. A flexible notification scheme and automated responses to critical events also aid in quick action.
- The event viewer can read both real-time and historical events.
- Events are color-coded and administrators can quickly isolate problems. Administrators can also define thresholds and time periods when rules can be triggered to provide notification.
- On-demand and scheduled reports facilitate ongoing monitoring.

For specific information on the security monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3991/index.html

VPN Monitoring

CiscoWorks VMS offers a Web-based management tool that allows network administrators to collect, store, and view information on IPsec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser. This dashboard provides the following capabilities:

- Provides data on system resources related to real-time memory usage, percent CPU usage per device, and active tunnel and active sessions. This data simplifies the identification of devices with potential performance problems and devices with the highest usage.
- Enables viewing of current and long-term packet rates and packet dropped percentage which can aid in determining where excess capacity can be tapped or quickly identify bottlenecks and device throughput problems.
- Enables identification of the devices with the most persistent problems through the event log; key device and VPN statistics are evaluated against a set of global and device-specific thresholds, and exceptions are recorded in the event log.
- Provides graphing of important common metrics. Device performance comparisons provide a global view of short-term trends in VPN performance, enabling administrators to identify problem areas before they become critical failures.

For specific information on the VPN monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2326/index.html

Operational Management

CiscoWorks VMS provides the operational management for the network, allowing network managers to perform the following:

- Quickly build a complete network inventory
- Manage device credentials information
- Monitor and report on hardware, software, configuration, and inventory changes
- Manage and deploy configuration changes and software image updates to multiple devices
- Monitor and troubleshoot critical LAN and WAN resources
- Quickly identify devices that can be used for VPNs, if upgraded with the appropriate Cisco IOS Software
- Discover which VPN devices have hardware encryption modules
- Graphically compare configurations of VPN devices
- Isolate IPsec-related problems by running customized Syslog reports

For specific information on the operational management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/index.html

Server Specifications (Minimum requirements)

Server Hardware

- PC-compatible computer with 1 GHz or faster Pentium processor
- Sun UltraSPARC 60 MP with 440 MHz or faster processor
- Sun UltraSPARCIII (Sun Blade 2000 Workstation or Sun Fire 280R Workgroup Server)

- CD-ROM drive
- 100BASE-T or faster connection
- 1 GB RAM
- 9 GB available disk drive space
- 2 GB virtual memory
- Color monitor with video card capable of 16-bit color

Server Operating System

CiscoWorks VMS requires the following operating systems:

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3)

Note: Support for Advanced Server requires that Terminal Services be turned off.

Sun Solaris 2.8 with patches:

109742 has been replaced by 108528-13

109322 has been replaced by 108827-15

109279 has been replaced by 108528-13

108991 has been replaced by 108827-15

Java Requirements

Sun Java plug-in 1.3.1-b24

Client Requirements

Hardware

- PC-compatible computer with 300 MHz or faster Pentium processor
- Solaris SPARCstation or Sun Ultra 10

Client Operating System

- Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM.
- Solaris 2.8

Client Browser

- Internet Explorer 6.0 Service Pack 1, on Windows operating systems
- Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP; Netscape Navigator 4.76 on Solaris 2.8

The CiscoWorks Management Center for Firewalls, and CiscoWorks Management Center for VPN Routers, are supported on Internet Explorer 6.0, but not on Netscape Navigator. In addition to supporting Internet Explorer The Management Center for IDS and the Monitoring Center for Security are also supported on Netscape Navigator.

6.186

Service and Support

CiscoWorks products are eligible for coverage under the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 24-hour access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A SAS contract ensures that customers have easy access to the information and services needed to stay current with newly supported device packages, patches, and minor updates. For further information about service and support offerings, contact your local sales office.

Ordering Information

CiscoWorks VMS is available for purchase through regular Cisco sales and distribution channels worldwide. CiscoWorks VMS includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris workstation.

For More Information

For more information, go to http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/ or send e-mail to ciscoworks@cisco.com

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

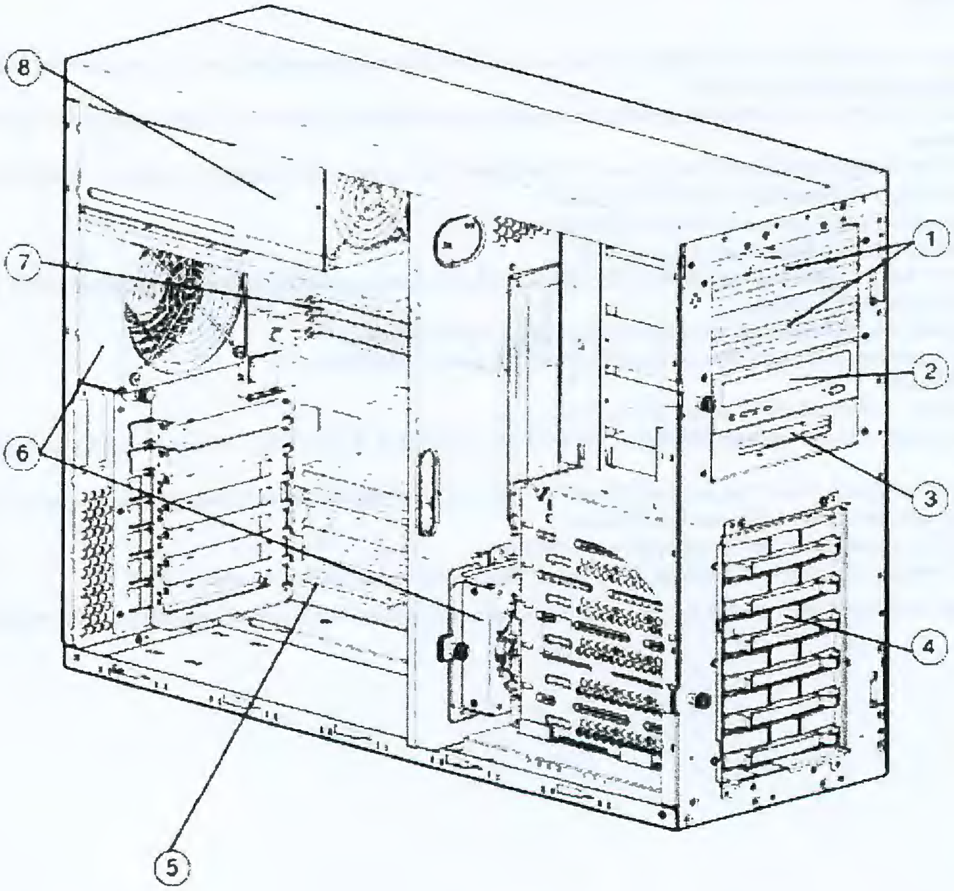
Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice EL

Overview



1. Two Removable Media Bays
2. 48X Max IDE (ATAPI) CD-ROM Drive
3. 1.44 Floppy Drive
4. Six 1" Hot Plug Drive Bays
5. Five expansion slots(four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI)
6. System fan
7. DIMM sockets for up to 8GB of memory, optionally interleaved
8. Optional 2nd Power Supply for hot-pluggable 1+1 redundancy

What's New

- Now available with Intel®Xeon 2.8 GHz Processors with 533MHz system bus.

At A Glance

- The ProLiant ML350 G3 is an expandable rack or tower platform delivering affordable 2-way performance and essential availability to corporate workgroups and growing businesses
- Intel Xeon 2.4 GHz or 2.8 GHz processors (dual processor capability) with 512-KB level 2 cache standard (full speed) and Hyper-Threading Technology
- ServerWorks Grand Champion LE Chipset with 533-MHz Front Side Bus for 2.8GHz processor models or 400-MHz FSB for models < 2.8 GHz
- Integrated Dual Channel Wide Ultra3 SCSI Adapter
- Smart Array Controller (standard in Array Models only)
- NC7760 PCI Gigabit Server Adapter (embedded)
- 512MB of 2-way interleaving capable PC2100 DDR SDRAM, with Advanced ECC capabilities (Array models only; 256MB standard on other models): Expandable to 8GB
- Flexible memory configurations allow interleaving (2x1) or non-interleaving
- Five available expansion slots: four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI
- Two USB ports
- Standard 6 x 1" Wide Ultra320 ready Hot Plug Drive Cage
- Internal storage capacity of up to 880GB (6 x 146.8 GB 1"), 1.174-TB (2 x 146.8 GB 1" + 6 x 146.8 GB 1") with optional 2-bay hot plug drive cage option
- 500W Hot-Pluggable Power Supply (standard) and an optional 500W Hot-Pluggable Redundant Power Supply (1+ 1) available
- Tool-free entry to chassis and access to components
- RBSU (ROM based setup utility) support, redundant ROM
- Insight Manager, SmartStart, ROM-based BIOS Setup Utility, and Automatic Server Recovery (ASR-2)
- Protected by HP Services, including a three-yeor, next business day, on-site, limited global warranty and extended Pre-Failure Warranty.

Standard Features

Processor *One of the following depending on Model:*	Intel Xeon Processor 2.8 GHz/533-512KB Intel Xeon Processor 2.4 GHz/400-512KB
Cache Memory	Integrated 512-KB Level 2 cache (full speed)
Upgradability	Upgradable to dual processing
Chipset	ServerWorks Grand Champion LE Chipset with 400-MHz or 533-MHz Front Side Bus (model dependent) NOTE: For more information regording ServerWorks, please see the following URL: http://www.serverworks.com/products/overview.html NOTE: This Web site is available in English only.

Memory
(One of the following depending on model)

2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advanced ECC capabilities

Standard (Non-Array Models)	256MB
Standard (Array Models)	512MB
Maximum	8 GB

Network Controller

NC7760 Gigabit Server Adapter (embedded)

Expansion Slots

I/O (5 Total, 5 Available)		PCI Voltage:
64-bit/100MHz, PCI	4 (4 available) (Array model has 3 available)	3.3 Volt or universal cards
32-bit/33MHz, PCI	1 (1 available)	5 Volt or universal cards

Storage Controller

Integrated Dual Channel Wide Ultra3 SCSI Adapter
Smart Array 641 Controller (2.8 GHz Array Models Only)

Storage

Diskette Drives	1.44 MB
CD-ROM	48x IDE (ATAPI) CD-ROM Drive
Hard Drives	None
Maximum Internal Storage	1.174 TB GB (6 x 146.8 GB 1" with standard internal hot plug drive cage + (2 x 146.8 GB 1") with optional ML3xx Two Bay Hot Plug SCSI Drive Cage)
External Storage	Two external SCSI knockouts available, optional ProLiant ML350 Internal to External SCSI Cable Option Kit required ● HD68 Internal to External SCSI Cable Option Kit PN 159547-B22 ● VHDCI Internal to External SCSI Cable Option Kit PN 333370-B21

Standard Features

Interfaces	Parallel	1
	Serial	1
	Pointing Device (Mouse)	1
	Graphics	1
	Keyboard	1
	Network RJ-45	1
	USB	2 NOTE: Please see the following URL for additional information regarding USB support: http://www.compaq.com/products/servers/platforms/usb-support.html. NOTE: This Web site is available in English only.
	External SCSI knockouts	2

Graphics	Integrated ATI RAGE XL Video Controller with 8-MB SDRAM Video Memory

Form Factor

Tower or rack (5U)

NOTE: Rack models (and rack conversion kit) support:

- Square hole racks from 27' - 32' deep (including Compaq/HP 7000, 9000, 10000 and H9 series)
- Square or round hole racks, from 24" - 35" deep (including HP Rack System /E and HP Systems, with an adjustment)
- Telco racks with 3rd part option kit from Rack Solutions

http://www.racksolutions.com/compaq/products.htm

NOTE: This Web site is available in English only.

Standard Features

ProLiant Essentials Foundation Pack Software

Insight Manager 7

Insight Manager 7 helps maximize system uptime and performance and reduces the cost of maintaining the IT infrastructure by providing proactive notification of problems before those problems result in costly downtime and reduced productivity. Insight Manager 7 is easy to set up and provides rapid access to detailed fault and performance information gathered by the Management Agents. One-click-access to the Remote Insight Lights Out Edition II board allows systems administrators to take full graphical control of ProLiant servers in remote locations or lights-out data centers. Finally, Insight Manager 7 in concert with the Version Control Agents and Version Control Repository Manager enables systems administrators to version manage and update system software across groups of ProLiant servers.

Management Agents

The Management Agents form the foundation for HP's Intelligent Manageability strategy. They provide direct, browser-based access to in-depth instrumentation built into HP servers, workstations, desktops, and portables, and send alerts to Insight Manager 7 and other enterprise management applications in case of subsystem or environmental failures. For additional information about the Management Agents and other management products from HP, please visit the management Web site at http://www.hp.com/servers/manage.

SmartStart

SmartStart is a tool that simplifies server setup, providing a rapid way to deploy reliable and consistent server configurations. For more information, please visit the SmartStart website at http://www.hp.com/servers/manage.
SmartStart version supported (minimum): SmartStart 5.50

ActiveUpdate

ActiveUpdate is a web-based application that keeps IT managers directly connected to HP for proactive notification and delivery of the latest software updates.

ROMPaq, support software, and configuration utilities

The latest software, drivers, and firmware fully optimized and tested for your ProLiant server and options.

Survey Utility and diagnostics utilities

The most advanced configuration analysis, reporting and troubleshooting utilities used by HP and at your fingertips.

Optional Proliant Essentials Value Packs

Optional software offerings that selectively extend the functionality of an Adaptive Infrastructure to address specific business problems and needs:

- Rapid Deployment Pack – an automated solution for multi-server deployment and provisioning, enabling companies to quickly and easily adapt to changing business demands.
- Workload Management Pack – provides easier management of complex environments, improving overall server utilization and enabling Windows 2000 customers for the first time to confidently deploy multiple applications on a single multiprocessor ProLiant Server.
- Performance Management Pack – a performance management solution that identifies and explains hardware performance bottlenecks on ProLiant servers and attached options enabling users to better utilize their valuable resources.

NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Value Packs. Refer to http://www.hp.com/servers/proliantessentials or the various ProLiant Essentials Value Pack product QuickSpecs for more information.
NOTE: For more information regarding ProLiant Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentials
NOTE: These Web sites are available in English only.

Industry Standard Compliance

ACPI V1.0B Compliant
PCI 2.2 Compliant
PXE Support
WOL Support
PCI-X 1.0 Compliant
Novell Certified
Microsoft Logo certifications

Standard Features

Manageability

Insight Manager 7
Redundant ROM
System Firmware Update
ROMPaq
Remote Insight Lights-Out Edition II (optional)
ProLiant RBSU (ROM-Based Setup Utility)
Automatic Server Recovery-2 (ASR-2)
Drive Parameter Tracking (with Smart Array Controller)
Dynamic Sector Repairing (with Smart Array Controller)
Pre-Failure Warranty (covers processors, memory and hard drives)

Security

Power-on password
Setup password
Diskette boot control
Parallel and serial interface control
Disk configuration lock
Power switch security

Server Power Cords

One Lowline NEMA power cord and one Highline IEC Power cord ship standard
Tower models ship with standard country specific power cords.
Rack models ship with IEC cables. Depending on the country, some also ship with country specific power cords
Redundant power supply options ship with country specific power cords with the exception of the -B21 Rack SKU which ships with an IEC cable only.

Power Supply

500 Watts, Power Factor Correction (PFC), Hot Plug 100 to 240 VAC Rated Input Voltage (Auto-sensing), CE Mark Compliant
Optional 2nd Power Supply for hot-pluggable 1 + 1 redundancy.

System Fans

2 fans ship standard, 2 fans total supported (does not include power supply fans)

Required Cabling

For required cabling information, refer to the HP Web site at http://www.hp.com/servers/proliantML350.
NOTE: This Web site is available in English only.

OS Support

Microsoft Windows NT® Server 4.0 and Terminal Server 4.0
Microsoft BackOffice Small Business Server 2000
Microsoft Windows 2000 Server and Advanced Server
Windows Server 2003
Novell NetWare 5.1, 6.0
Novell NetWare Small Business Suite 6.0
SCO OpenServer 5.0.6a
SCO OpenUnix 8 SCO UnixWare 7.1.1
IBM OS/2 Warp Server for e-business
LINUX (Red Hat, 2.1 Advanced Server, Red Hat 8.0 and Red Hat 7.3, SuSE, SLES7, UnitedLinux 1.0)
NOTE: For a more complete and up-to-date listing of supported OSs and versions, please visit our OS Support Matrix at: ftp://ftp.compaq.com/pub/products/servers/os-support-matrix-310.pdf
NOTE: Optional hardware may be required to support some operating systems.
NOTE: For an up-to-date listing of the latest drivers available for the ProLiant ML350, please see: http://www.compaq.com/support/files/server/us/index.html.
NOTE: These Web sites are available in English only.

Rack Airflow Requirements

- Rack 9000 and 10000 series Cabinets
  The increasing power of new high-performance processor technology requires increased cooling efficiency for rack-mounted servers. The 9000 and 10000 Series Racks provide enhanced airflow for maximum cooling, allowing these racks to be fully loaded with servers using the latest processors.
- Rack 7000 series Cabinets
  When installing a server with processors running at speeds of 550 MHz or greater in Rack 7000 series racks with glass doors (165753-001 (42U), and 163747-001 (22U)), the new processar technology requires the installation of HP's new High Airflow Rack Door Inserts (327281-B21 (42U), 327281-B22 (42U 6 pack), or 157847-B21 (22U)) to promote enhanced airflow for maximum cooling.

CAUTION: If a third-party rack is used, observe the following additional requirements to ensure adequate airflow and to prevent damage to the equipment:

- ○ Front and rear doors: If your 42U server rack includes closing front and rear doors, you must allow 830 square inches (5,350 sq cm) of hole evenly distributed from top to bottom to permit adequate airflow (equivalent to the required 64 percent open area for ventilation).
- ○ Side: The clearance between the installed rack component and the side panels of the rack must be a minimum of 2.75 inches (7 cm).

CAUTION: Always use blanking panels to fill all remaining empty front panel U-spaces in the rock. This arrangement ensures proper airflow. Using a rack without blanking panels results in improper cooling that can lead to thermal damage.

NOTE: For additional information, refer to the Setup and Installation Guide or the Documentation CD provided with the server, or to the server documentation located in the Support section at the following URL:
http://www5.hp.com/servers/proliantml350
NOTE: This Web site is available in English only.

Installation of Server into Telco Racks

ML350 G3 rack model support: Support for all 2-post Telco racks requires the use of the rack kit and an additional option kit from Rack Solutions. http://www.racksolutions.com/compaq
NOTE: This Web site is available in English only.

HP Factory Express Capabilities

HP Factory Express gives you the flexibility to choose from a full menu of factory capabilities all in one manufacturing facility, in one process, with one touch giving you full control and access to HP's World class manufacturing facility anytime. This approach provides you the speed to deploy your IT needs, with total quality assurance, reliability, and predictability to lower your total cost of ownership by letting HP install, rack, and customize your software and hardware options for you.

Service and Support

HP Services provides a three-year, limited warranty, including Pre-Failure Warranty (coverage of hard drives, memory and processors) fully supported by a worldwide network of resellers and service providers and lifetime toll-free 7 x 24 hardware technical phone support. In addition, available service offerings include:
NOTE: Limited Warranty includes 3 year Parts, 3 year Labor, 3-year on-site support.

A full range of HP Care Pack packaged hardware and software services:

- Installation and start up
- Extended coverage hours and enhanced response times
- System management and performance services
- Availability and recovery services

NOTE: For more infomation, visit http://www.hp.com/services/carepack.

Please see the following URL regarding Warranty Information For Your HP Products:
http://www.compaq.com/support/warranty_upgrades/web_statements/176738.html.

For additional information regarding Worldwide Limited Warranty and Technical Support, please see the following URL:
ftp://ftp.compaq.com/pub/supportinformation/ejourney/176738.pdf.
NOTE: These Web sites are available in English only.

NOTE: Certain restrictions and exclusions apply. Consult the Customer Support Center at 1-800-345-1518 for details.

Models

ML350T03 X2.8-512KB/533, 256MB *311523-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)

ML350R03 X2.8-512KB/533, 256MB *311524-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

ML350T03 X2.8-512KB/533, 512MB Array *311525-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)

ML350R03 X2.8-512KB/533, 512MB Array *311526-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB of Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

Models

ML350T03 X2.4-512KB/400, 256MB *269786-001*	Processor(s)	(1) Intel Xeon Processor 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)

ML350R03 X2.4-512KB/400, 256MB *269787-001*	Processor(s)	(1) Xeon 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drives & drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

Options

ProLiant ML350 G3 Unique Options	Hot Plug Redundant Power Supply Option Kit	283655-001
	Hot Plug Redundant Power Supply Option Kit (cable) NOTE: PN 283655-B21 SKU contains the 2nd power supply with an IEC power cable. Only purchase if connecting to PDU/UPS that supports IEC cables. All other SKUs contain country specific power cables.	283655-B21
	Intel Xeon 2.80 GHz-512KB Processor Option Kit NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiant ML350 G3 systems with 533 MHz front side bus only. This kit cannot be used in 400 MHz front side bus systems such as those with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	314763-B21
	Intel Xeon 2.40 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 257913-B21) supports the ProLiant ML350 G3 servers.	257913-B21
	Intel Xeon 2.20 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 283702-B21) supports the ProLiant ML350 G3 servers.	283702-B21
	Intel Xeon 2.0 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 283701-B21) supports the ProLiant ML350 G3 servers.	283701-B21
	ProLiant ML350 G3 Tower to Rack Conversion Kit (CPQ brand)	290683-B21
ProLiant Essentials Value Pack Software	Rapid Deployment Pack, 1 User, V1.x NOTE: This license allows 1 server to be managed and deployed via the Deployment Server.	267196-B21
	Rapid Deployment Pack, 10 Users, V1.x NOTE: This license allows 10 servers to be managed and deployed via the Deployment Server.	269817-B21
	Flexible Quantity License Kit	302127-B21
	License-Only - for use with a Master License Agreement	302128-B21
	ProLiant Essentials Workload Management Pack 2.0 (Featuring Compaq Resource Partitioning Manager version 2.0)	303284-B21
	ProLiant Essentials Performance Management Pack Flexible License	306697-B21
	NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Value Packs. Refer to http://www.hp.com/servers/proliantessentials or the various ProLiant Essentials Value Pack product QuickSpecs for more information. NOTE: For more information regarding ProLiant Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentials. NOTE: These Web sites are available in English only.	
HP NetServer Transition Services	HP NetServer to ProLiant integration and assessment service NOTE: HP identifies current levels of NetServer support, services, and management. This service helps maximize customer's ability to add ProLiant platforms into their current environment.	304164-002
	HP TopTools to Insight Manager 7 installation and startup service NOTE: Provides on-site review, installation and configuration services for Insight Manager 7. HP will also re-create, as closely as possible, the views and reports from the customer's current TopTools configuration. This service assures a smooth transition to the ProLiant Essentials software.	304163-002
	HP NetServer to ProLiant Essentials Rapid Deployment Pack installation and startup service NOTE: Install and configure Rapid Deployment Pack in a test environment, then deploy a server image to a maximum of 250 systems in the production environment. This service helps to assure successful system deployment.	304162-002

Processors	Intel Xeon 2.80 GHz-512KB Processor Option Kit NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiant ML350 G3 systems with 533 MHz front side bus only. This kit cannot be used in 400 MHz front side bus systems such as thhose with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	314763-B21
	Intel Xeon 2.40 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 257913-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	257913-B21
	Intel Xeon 2.20 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283702-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	283702-B21
	Intel Xeon 2.0 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283701-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	283701-B21
Memory (DIMMs)	NOTE: The ML350 G3 supports both interleaved and non-interleaved memory configurations. Base models ship standard with one 256MB DIMM or one 512MB DIMM (Array models). For best performance automatically invoke interleaving by populating memory in identical pairs. If 1GB of total memory is desired odd three 256MB DIMMs to the base configuration. If 1.5GB of memory is desired add one 256MB DIMM (to pair with the standard DIMM) and two 512MB DIMMs. Interleaving and installation of memory in pairs is not required. Add any combination of memory DIMMs below to operate in non-interleaved mode. NOTE: Each SDRAM Memory kit contains one (1) DIMM.	
	128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
	256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21
	512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21
	1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
	2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21
Internal Storage	ML3xx Two Bay Hot Plug SCSI Drive Cage NOTE: The drive cage option kit (PN 244059-B21) has one 1" drive bay and one 1.6" drive bay. It installs in two available removable media bays.	244059-B21
Optical Drives	16X DVD-ROM Drive Option Kit (Carbon)	217053-B21
	CD-RW/DVD-ROM 48X Combo Drive Option Kit	3[illegible]6-B21
Hard Drives	*Ultra320 – Universal Hot Plug*	
	146.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286716-B22
	72.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286714-B22
	36.4-GB 10,000 rpm U320 Universal Hard Drive (1")	286713-B22
	72.8-GB 15,000 rpm U320 Universal Hard Drive (1")	286778-B22
	36.4-GB 15,000 rpm U320 Universal Hard Drive (1")	286776-B22
	18.2-GB 15,000 rpm U320 Universal Hard Drive (1")	286775-B22
	NOTE: All U320 Universal Hard Drives are backward compatible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates	
	NOTE: Please see the Wide Ultra320 Universal Hot Plug QuickSpecs for additional technical information on the hard drives Support details, please see the following: http://www.compaq.com/products/quickspecs/[illegible]531[illegible]53[illegible]	

Options

Storage Controllers	Smart Array 6402/128 Controller	273915-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Compaq RAID LC2 Controller	188044-B21
	Smart Array 532 Controller	225338-B21
	Smart Array 5302/128 Controller	283552-B21
	Smart Array 5304/256 Controller	283551-B21
	Smart Array 5312 Controller	238633-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Ultra3 Channel Expansion Module for Smart Array 5300 Controller	153507-B21
	128-MB Cache Module for Smart Array 5302 Controller	153506-B21
	RAID ADG Upgrade for Smart Array 5302	288601-B21
	256-MB Battery Backed Cache Module NOTE: This 256-MB Battery Backed Cache Module supports the Smart Array 5300 series controllers, MSA 1000 and the Smart Array Cluster Storage.	254786-B21
	256MB Cache Upgrade for SA-6402 NOTE: This 256-MB Battery-Backed Cache Module upgrade kit supports the Smart Array 6400 series controller only.	273913-B21
	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS	284688-B21
	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter	268351-B21
	NOTE: Please see the following Controller or SCSI Adapter QuickSpecs for Technical Specifications such as PCI Bus, PCI Peak Data Transfer Rate, SCSI Protocols supported, SCSI Peak Data Transfer Rate, Channels, SCSI Ports, Drives supported, Cache, RAID support, and additional information: http://www5.compaq.com/products/quickspecs/10652_na/10652_na.HTML (RAID LC2) http://www5.compaq.com/products/quickspecs/10851_na/10851_na.HTML (Smart Array 532) http://www5.compaq.com/products/quickspecs/10640_na/10640_na.HTML (Smart Array 5300 Series) http://www5.compaq.com/products/quickspecs/11328_na/11328_na.HTML (Smart Array 5312) http://www5.compaq.com/products/quickspecs/11587_na/11587_na.HTML (Smart Array 6402) http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML (Smart Array 641) http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML (Smart Array 642) http://www5.compaq.com/products/quickspecs/10429_na/10429_na.HTML (SCSI Adapter) http://www5.compaq.com/products/quickspecs/11555_nav/11555_na.HTML (U320 Adapter)	
Wireless HAP Solution	Compaq WL410 Wireless SMB Access Point	191811-001

6-172

Options

Communications	NC3123 Fast Ethernet NIC PCI 10/100 WOL and PXE	174830-B21
	NC3134 Fast Ethernet NIC 64 PCI Dual Port 10/100	138603-B21
	NC3135 Fast Ethernet Module Dual 10/100 Upgrade Module for NC3134	138604-B21
	NC6132 1000 SX Upgrade Module for NC3134	338456-B23
	NC6136 Gigabit Server Adapter, 64-bit/66MHz, PCI, 1000 SX	203539-B21
	NC6170 Dual Port PCI-X 1000SX Gigabit Server Adapter	313879-B21
	NC6770 PCI-X Gigabit Server Adapter, 1000-SX	244949-B21
	NC7170 Dual Port PCI-X 1000T Gigabit Server Adapter	313881-B21
	NC7132 Gigabit Upgrade Module 10/100/1000-T	153543-B21
	NC7770 PCI-X Gigabit server adapter	244948-B21
	56K v.90 PCI Modem	239137-001
	NOTE: Any NC31XX, NC61XX, NC71XX or NC77XX NIC can be used for redundancy with the embedded NC7760 Network Controller.	
Management Options	Remote Insight Lights-Out Edition II	227251-001
Security	HP/Atalla AXL600L SSL Accelerator Card for ProLiant Servers	524545-B21
Monitors	*Essential Series*	
	Compaq S9500 CRT Monitor (19-inch, Carbon/Silver)	261615-003
	Compaq S7500 CRT Monitor (17-inch, Carbon/Silver)	261606-001
	Compaq S5500 CRT Monitor (15-inch Carbon/Silver)	261602-001
	Compaq TFT1501 Flat Panel Monitor (15-inch, Carbon/Silver)	301042-003
	Compaq TFT1701 Flat Panel Monitor (17-inch, Carbon/Silver)	292847-003
	Advantage Series	
	Compaq V7550 CRT Color Monitor (17-inch, Carbon/Silver)	261611-003
	Compaq TFT1720 Flat Panel Monitor (17-inch, Carbon/Silver)	295926-003
	Compaq FT1720M Flat Panel Monitor (17-inch, Carbon/Silver, includes speaker, USB port, headphone)	301958-003
	Compaq TFT1520 Flat Panel Monitor (15-inch, Carbon/Silver)	295925-003
	Compaq TFT1520M Flat Panel Monitor (15-inch, Carbon/Silver includes speaker, USB port, headphone)	301957-003
	Performance Series	
	HP P930 CRT Monitor (19-inch, Flat-screen, Carbon/Silver)	302268-003
	HP P1130 CRT Monitor (21-inch, Flat-screen, Carbon/Silver)	302270-003
	HP L1825 Flat Panel Monitor (18-inch, Carbon/Silver)	303486-003
	HP L2025 Flat Panel Monitor (20-inch, Carbon/Silver)	303102-003
	Compaq TFT1825 Flat Panel Monitor (18-inch, Carbon/Silver)	296751-003
	Compaq TFT2025 Flat Panel Monitor (20-inch, Carbon/Silver)	285550-003
	Rackmount Flat Panel Monitors	
	TFT5110R Flat Panel Monitor (Carbon)	281683-B21
	NOTE: Monitors larger than 17" may be too heavy for use in rack systems.	

Options

Tape Drives

NOTE: In order to install certain tape drives internally, you may need to remove the rails that come standard on the drives and then re-insert the screws in the mounting holes. To ensure proper fit, install the mounting screws as described in the tape option kit.

Internal and External DAT Tape Drives

Internal 12/24-GB DAT Drive (Opal)	295513-B22

NOTE: Please see the 12/24-GB DAT Drive QuickSpecs for additional options such as cassettes and for on up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10239_na/10239_na.HTML

HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, Internal (Carbon)	157769-B22
HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, External (Carbon)	157770-002
HP StorageWorks Internal 20/40-GB DAT, Hot Plug (Carbon)	215488-B21

NOTE: Please see the 20/40-GB DAT Tape Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for on up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10426_na/10426_na.HTML

Internal and External DAT 72 Tape Backup Drive

HP StorageWorks DAT 72 Tape Drive Internal (Carbon)	Q1525A
HP StorageWorks DAT 72 Tape Drive, External (Carbon)	Q1527A
HP StorageWorks DAT 72h Internal Hot Plug (Carbon)	Q1529A

NOTE: Please see the DAT 72 Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for on up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11597_na/11597_na.HTML

Internal and External LTO Ultrium Tape Drives

HP StorageWorks Ultrium 215 Tape Drive for ProLiant, Internal (Carbon)	Q1543A
HP StorageWorks Ultrium 215 Tape Drive for ProLiant, External (Carbon)	Q1544A

NOTE: Please see the HP StorageWorks Ultrium 230 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for on up-to-date listing of the latest O/S Support details, please see the following:
http://h18006.www1.hp.com/products/quickspecs/11678_na/11678_na.html

HP StorageWorks LTO Ultrium 230 Tape Drive, Internal (Carbon)	Q1515A
HP StorageWorks LTO Ultrium 230 Tape Drive, External (Carbon)	Q1516A

NOTE: Please see the HP StorageWorks LTO Ultrium QuickSpecs for additional options such as data and cleaning cartridges, and for on up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11415_na/11415_na.HTML

HP StorageWorks Ultrium 460 tape drive for ProLiant, Internal (Carbon)	Q1518A
HP StorageWorks Ultrium 460 tape drive for ProLiant, External (Carbon)	Q1519A

NOTE: Please see the HP StorageWorks Ultrium 460 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for on up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11530_na/11530_na.HTML

Internal and External AIT Tape Drives

NOTE: The Internal AIT Hot Plug Drives are supported in hot plug drive bays only. When installing a non hot plug AIT tape drive into an ML350 ProLiant server use the special screw included with the drive kit proper fit in the removable media bay.

HP StorageWorks Internal AIT 35-GB, LVD Tape Drive (Carbon)	216884-B21
HP StorageWorks External AIT 35-GB, LVD Tape Drive (Carbon)	216885-001
HP StorageWorks Internal AIT 35-GB, LVD, Hot Plug (Carbon)	216886-B21

NOTE: Please see the AIT 35-GB, LVD Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10712_na/10712_na.HTML

HP StorageWorks AIT 50-GB Tape Drive, Internal (Carbon)	157766-B22
HP StorageWorks AIT 50-GB Tape Drive, External (Carbon)	157767-002
HP StorageWorks Internal AIT 50-GB, Hot Plug (carbon)	215487-B21
HP StorageWorks Rackmount AIT 50-GB, 3U (Single Drive)	274333-B21

NOTE: Please see the AIT 50-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10425_na/10425_na.HTML

HP StorageWorks Internal AIT 100-GB Tape Drive (Carbon)	249189-B21
HP StorageWorks External AIT 100-GB Tape Drive (Carbon)	249160-001
HP StorageWorks Internal AIT 100-GB, Hot-Plug (Carbon)	249161-B21

NOTE: Please see the AIT 100-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11062_na/11062_na.HTML

Internal and External DLT/SDLT Tape Drives

NOTE: When installing a DLT or SDLT tape drive into a ProLiant ML350, use the special screw included with the drive kit to ensure proper fit in the removable media bay.

HP StorageWorks 40/80-GB DLT Tape Drive, Internal (Carbon)	146196-B22
HP StorageWorks 40/80-GB DLT Tape Drive, External (Carbon)	146197-B23
HP StorageWorks Rackmount DLT 40/80, 3U (Single Drive)	274332-B21
HP StorageWorks Rackmount DLT 40/80, Dual-Drive, 3U (Two Drives)	274335-B21
HP StorageWorks Rackmount DLT 40/80, Tape Array III, 5U (Four Drives)	274337-B21

NOTE: Please see the 40/80-GB DLT Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10658_na/10658_na.HTML

HP StorageWorks DLT VS 40/80 Tape Drive, Internal (Carbon)	280129-B21
HP StorageWorks DLT VS 40/80 Tape Drive, External (Carbon)	280129-B22

NOTE: Please see the 40/80-GB DLT VS Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11403_na/11403_na.HTML

HP StorageWorks SDLT 110/220, Internal (carbon)	192106-B25
HP StorageWorks SDLT 110/220, External (Carbon)	192103-002
HP StorageWorks Rackmount SDLT 110/220, 3U (Single Drive)	274331-B21
HP StorageWorks Rackmount SDLT 110/220, Dual-Drive, 3U (Two Drives)	274334-B21
HP StorageWorks Rackmount SDLT 110/220, Tape Array III, 5U (Four Drives)	274336-B21

NOTE: Please see the SDLT 110/220-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10772_na/10772_na.HTML

HP StorageWorks SDLT 160/320, Internal (carbon)	257319-B21
HP StorageWorks SDLT 160/320, External (carbon)	257319-001

NOTE: Please see the SDLT 160/320GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11406_na/11406_na.HTML

Internal and External DAT Autoloader

20/40-GB DAT 8 Cassette Autoloader Internal (Opal)	166504-B21
20/40-GB DAT 8 Cassette Autoloader External (Opal)	166505-001

NOTE: Please see the 20/40-GB DAT DDS-4 8 Cassette Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10518_na/10518_na.HTML

AIT Autoloader

HP StorageWorks AIT 35GB Autoloader, Rackmount (carbon)	280349-001
HP StorageWorks AIT 35GB Autoloader Tabletop (carbon)	292355-001

NOTE: Please see the HP StorageWorks AIT 35GB Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11404_na/11404_na.HTML

HP StorageWorks 1/8 Autoloader

HP StorageWorks 1/8 Autoloader, Tabletop, Ultrium 230	C9572CB
HP StorageWorks 1/8 Autoloader, Tabletop, DLT VS80	C9264CB
HP StorageWorks 1/8 Autoloader, Rackmount kit	C9266R

NOTE: Please see the HP StorageWorks 1/8 Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11496_na/11496_na.HTML

SSL1016 tape autoloader

SSL1016 DLT1 tape autoloader (includes two 8-cartridge magazines and a barcode reader)	3308[illegible]21

NOTE: Please see the SSL1016 DLT1 tape autoloader Quick Specs for additional information:
http://h18000.www1.hp.com/products/quickspecs/11626_na/11626_na.HTML

SSL1016 SDLT 160/320 tape autoloader (includes two 8-cartridge magazines and a barcode reader)	330816-B21

NOTE: Please see the SSL1016 SDLT160/320 tape autoloader Quick Specs for additional information:
http://h18000.www1.hp.com/products/quickspecs/11609_na/11609_na.HTML

Add-on drives and accessories

SSL1016 DLT/SDLT 8-cartridge magazine	268664-B22

Rackmount Tape Drive Kits

3U Rackmount Kit	274338-B21

NOTE: The 3U Rackmount Kit (PN 274338-B21) can support up to (2) full-height or (4) half-height tape drives and compatible with multiple Single-Ended and LVD SCSI Tape Drives including the 12/24-GB DAT, 20/40-GB DAT, DAT 72-GB, 20/40-GB DAT DDS-4 8 Cassette Autoloader, AIT 35GB LVD, AIT 50GB, AIT 100-GB, 40/80-GB DLT, DLT VS 40/80-GB, SDLT 110/220-GB, SDLT 160/320-GB, Ultrium 215, Ultrium 230 and Ultrium 460 Tape Drives.

5U Rackmount Kit	274339-B21

NOTE: The 5U Rackmount Kit (PN 274339-B21) can support up to (4) full-height tape drives and is compatible with DLT/SDLT/LTO tape drives including the 40/80-GB DLT, SDLT 110/220, SDLT 160/320, Ultrium 230, and Ultrium 460 Tape Drives.

NOTE: Please see the Rackmount Tape Drive Kits QuickSpecs for additional information regarding these kits, please see the following:
http://www5.compaq.com/products/quickspecs/10854_na/10854_na.HTML

Tape Storage Enclosure Cable Kits

LVD Cable Kit, VHDCI/HD68	168048-B21

NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Array III only.

LVD Cable Kit, HD68/HD68	242381-B21

NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Array III only.

Options

Tape Automation

StorageWorks SSL2000 small system library

SSL2020 – AIT50 based library with up to 2 drives and 20 slots

SSL2020 AIT Mini-Library 1 drive, 20 slot Table Top	175195-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Table Top	175195-B22
SSL2020 AIT Mini-Library 1 drive, 20 slot Rackmount	175196-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Rackmount	175196-B22
SSL2020 AIT Library Pass Thru with Transport	175312-B21

Add-on drives and accessories

SSL2020 AIT Library Pass Thru Extender	175312-B22
AIT 50GB Drive Add-On LVD Drive for SSL2020 AIT Library	175197-B21
19 Slot Magazine for SSL2020 AIT Library	175198-B21
AIT 50-GB Data Cassette (5 pack)	152841-001
AIT Cleaning Cassette	402374-B21

NOTE: Please see the SSL2020 Automated AIT Tape Library Solution QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10580_na/10580_na.HTML

StorageWorks MSL6000 and MSL5000 Departmental tape libraries

MSL6060L1 – Ultrium 460 1 based departmental library up to 4 drives and 60 slots

MSL6060L1, 0 DRV Ultrium 460 RM Library	331196-B23
MSL6060L1, 2 DRV Ultrium 460 RM Library	331195-B21
MSL6060L1, 2 DRV Ultrium 460 TT Library	331196-B21
MSL6060L1FC, 2 DRV Ultrium 460 embedded Fibre RM Library	331196-B22

NOTE: Please see the StorageWorks MSL6060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11608_na/11608_na.HTML

StorageWorks MSL6000 and MSL5000 departmental libraries

MSL5060L1 – LTO Ultrium 1 based departmental library up to 4 drives and 60 slots

MSL5060L1, 0 DRV LTO1 RM Library	301899-B21
MSL5060L1, 2 DRV LTO1 RM Library	301899-B22
MSL5060L1, 2 DRV LTO1 TT Library	301900-B21
MSL5060L1FC, 2 DRV LTO1 RM-with integrated FC router	301899-B23

NOTE: Please see the StorageWorks MSL5060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11438_na/11438_na.HTML

MSL5052S2 – SDLT160 based departmental library up to 4 drives and 52 slots

MSL5052S2, RM 0 DRV SDLT ALL	255102-B21
MSL5052S2, 2 DRV SDLT2 TT LIB	293476-B21
MSL5052S2, 2 DRV SDLT2 RM LIB	293474-B21
MSL5052S2FC 2 DRV SDLT2 RM- with integrated FC router	293474-B24

NOTE: Please see the StorageWorks MSL5052S2 Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11442_na/11442_na.HTML

6468

MSL6030 – LTO Ultrium 460 mid-range library up to 2 drives and 30 slots

MSL6030 0-drive, LTO, LVDS, RM	330731-B21
MSL6030 1-drive, LTO Gen2, LVDS, RM	330731-B22
MSL6030 2-drive, LTO Gen2, LVDS, RM	330731-B23
MSL6030 1-drive, LTO Gen2, Fibre, RM	330731-B24
MSL6030 2-drive, LTO Gen2, Fibre, RM	330731-B25
MSL6030 1-drive, LTO Gen2, LVDS, TT	330788-B21
MSL6030 2-drive, LTO Gen2, LVDS, TT	330788-B22

MSL5030L1 – LTO Ultrium 1 mid-range library up to 2 drives and 30 slots

MSL5030L1, 0 DRV LTO1 RM Library	301897-B21
MSL5030L1, 1 DRV LTO1 RM Library	301897-B22
MSL5030L1, 2 DRV LTO1 RM Library	301897-B23
MSL5030L1, 1 DRV LTO1 TT Library	301898-B21
MSL5030L1, 2 DRV LTO1 TT Library	301898-B22
MSL5030L1FC, 1 DRV LTO1 RM- with integrated FC router	301897-B24

NOTE: Please see the StorageWorks MSL5030 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11439_na/11439_na.HTML

MSL5026S2 – SDLT160 based mid-range library up to 2 drives and 26 slots

MSL5026S2, 0 DRV SDLT2 RM Library	293472-B21
MSL5026S2, 1 DRV SDLT2 RM Library	293472-B22
MSL5026S2, 2 DRV SDLT2 RM Library	293472-B23
MSL5026S2, 1 DRV SDLT2 TT Library	293473-B21
MSL5026S2, 2 DRV SDLT2 TT Library	293473-B22
MSL5026S2FC, 1 DRV SDLT2 RM- with integrated FC router	293472-B24
MSL5026S2FC, 2 DRV SDLT2 RM- with integrated FC router	293472-B25

NOTE: Please see the StorageWorks MSL5026SL Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11453_na/11453_na.HTML

MSL5026SL Graphite – SDLT110 based mid-range library up to 2 drives and 26 slots

MSL5026SL, 1 DRV SDLT TT, graphite	302511-B21
MSL5026SL, 2 DRV SDLT TT, graphite	302511-B22
MSL5026SL, 1 DRV SDLT RM, graphite	302512-B21
MSL5026SL, 2 DRV SDLT RM, graphite	302512-B22

NOTE: Please see the StorageWorks MSL5026SL Graphite Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11440_na/11440_na.HTML

MSL5026DLX– 40/80GB DLT based mid-range library up to 2 drives and 26 slots

MSL5026DLX, 1 40/80GB DLT, LVD, TT	231821-B21
MSL5026DLX, 2 40/80GB DLT, LVD, TT	231821-B22
MSL5026DLX, 1 40/80GB DLT, LVD, RM	231891-B21
MSL5026DLX, 2 40/80GB DLT, LVD, RM	231891-B22

NOTE: Please see the StorageWorks MSL5026DLX Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10860_na/10860_na.HTML

MSL6000 and MSL5000 Add-on drives & accessories

MSL SDLT 160/320 Upgrade DRV	293475-B21
MSL Ultrium 460 upgrade drive in hot plug canister	330729-B21
MSL5000 SDLT 110/220 Upgrade DRV	231823-B22
MSL5000 40/80GB DLT Upgrade DRV	231823-B21
MSL Dual Magazine DLT (2 X 13 slot magazines)	232136-B21
MSL Universal passthrough mechanism	304825-B21
MSL 5U passthrough extender	231824-B22
MSL 10U passthrough extender	231824-B23
MSL Dual Magazine - Ultrium	301902-B21

6.164

Options

Smart Array Cluster Storage	Smart Array Cluster Storage	201724-B21
	Smart Array Cluster Storage Redundant Controller Option Kit	218252-B21
	128MB Cache Module for Smart Array 5302 Controller	153506-B21
	256MB Battery Backed Cache Module	254786-B21
	4-Port Shared Storage Module with Smart Array Multipath Software for Smart Array Cluster Storage	292944-B21
	NOTE: All 128MB Cache modules must be removed when 256MB cache modules are installed. NOTE: Please see the Smart Array Cluster Storage QuickSpecs for additional information including configuration steps and additional options needed for a complete solution at: http://www5.compaq.com/products/quickspecs/11050_na/11050_na.html	
External Storage – Tower and Rack	StorageWorks Enclosure Model 4314T (tower)	190210-001
	StorageWorks Enclosure Model 4314R (rack-mountable)	190209-001
	StorageWorks Enclosure Model 4354R (rack-mountable)	190211-001
	NOTE: The StorageWorks Enclosure 4300 Family support the Wide Ultra2/Ultra3 1" Hot Plug Hard Drives.	
	Redundant Power Supply Option	1198[illegible]21
	Ultra3 Single Bus I/O Module Option	1902[illegible]B21
	Ultra3 Dual Bus I/O Module Option	190213-B21
	StorageWorks Enclosure Tower to Rack Conversion Kit	150213-B21
MSA1000	MSA1000	201723-B22
	MSA1000 Controller	218231-B22
	MSA Fibre Channel I/O Module	218960-B21
	MSA1000 Fabric Switch	218232-B21
	MSA1000 Fibre Channel Adapter (FCA) 2101	245299-B21
	HP StorageWorks msa hub 2/3	286763-B21
	NOTE: Please see the StorageWorks by Compaq Modular SAN Array 1000 QuickSpecs for additional options and configuration information at: http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML	
Network Storage Router	M2402 2FCX 4SCSI LVD Network Storage Router	262653-B21
	M2402 2FCX 4SCSI HVD Network Storage Router	262654-B21
	M2402 4 channel LVD SCSI Module	2626[illegible]21
	M2402 4 channel HVD SCSI Module	2626[illegible]B21
	M2402 2 channel FC Module	262661-B21
	MSL5000 Embedded Router Fibre Option Kit - Graphite	262672-B21
	MSL5026 Embedded Router Fibre Option Kit - Opal	286694-B21
StorageWorks Options	StorageWorks Fibre Channel SAN Switches 8-EL	176219-B21
	StorageWorks SAN Switch 2/8-EL	258707-B21
	StorageWorks SAN Switch 2/16-EL	283056-B21
	StorageWorks SAN Switch 2/8-EL Upgrade Kit	288162-B21
	StorageWorks SAN Switch 2/16-EL Upgrade Kit	288250-B21

Options

UPS and PDU Power Cord Matrix	Please see the UPS and PDU cable matrix that lists cable descriptions, requirements, and specifications for UPS and PDU units: ftp://ftp.compaq.com/pub/products/servers/ProLiantstorage/power-protection/powercordmatrix.pdf. NOTE: This Web site is available in English only.	
Uninterruptible Power Systems – Tower UPSs	HP UPS Model T700 (700VA, 500 Watt), Low Voltage	204015-001
	HP UPS T1000 XR (1000 VA, 700 Watts), Low Voltage	204155-001
	HP UPS T1500 XR (1440 VA, 1050 Watts)	204155-002
	HP UPS T2200 XR (1920 VA, 1600 Watts) Low Voltage	204451-001
	HP UPS T2200 XR (2200 VA, 1600 Watts) High Voltage	204451-002
Uninterruptible Power Systems – HP Rack UPSs	HP UPS R1500 XR (100 to 127)	204404-001
	HP UPS R3000 XR (120V)	192186-001
	HP UPS R3000 XR (208V)	192186-002
	Rack-Mountable UPS R6000 (208V) NOTE: UPS R6000 has a hardwired input; and the UPS R12000 XR has a hardwired input and output connection.	347207-001
	HP UPS R12000 XR N+ x (200-240V) NOTE: The UPS R12000 XR has a hardwired input and output. NOTE: HP UPS R6000 has a hardwired input; the UPS R12000 XR has a hardwired input and output connection.	207552-B22
UPS Options	SNMP Serial Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 – 3000VA	192189-B21
	Six Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 – 3000VA.	192185-B21
	High to Low Voltage Transformer (250VA) NOTE: Supports R6000 UPS series only. 2.5A @ 125 Volts max output across two NEMA 5-15.	388643-B21
	Extended Runtime Module, T1000 XR	218967-B21
	Extended Runtime Module, T1500 XR/T2200 XR	218969-B21
	Extended Runtime Module, R1500 XR NOTE: 2U each, two ERM maximum.	218971-B21
	Extended Runtime Module, R3000 XR NOTE: 2U each, one ERM maximum.	192188-B21
	Extended Runtime Module, R6000 NOTE: 3U each, two ERM maximum.	347224-B21
	Extended Runtime Module, R12000 XR, 4U each, two ERMs maximum	217800-B21
	R12000 XR BackPlate Receptacle Kit, (2) L6-30R NOTE: The R12000 XR BackPlate Kit has a hardwired input.	325361-001
	R12000 XR BackPlate Receptacle Kit, (2) IEC-309R NOTE: The R12000 XR BackPlate Kit has a hardwired input	325361-B21
	SNMP-EN Adapter NOTE: Supports R6000 UPS series only.	347225-B21
	Multi-Server UPS Card NOTE: Supports R6000 UPS series only.	123508-B21
	Scalable UPS Card NOTE: Supports R6000 UPS series only	123509-B21

Options

Modular PDUs 1U/0U (Up to 32 outlets) NOTE: 1U/0U mounting brackets shipped with the unit (optimized for 10000 and 9000 series racks).	HP Modular Power Distribution Units (mPDU), Low Volt Model, 24A (100-127 VAC)	252663-D71
	NOTE: This mPDU (252663-D71) may also be used to connect the low volt model of the UPS R3000 XR.	
	HP Modular Power Distribution Units (mPDU), High Volt Model, 24A (200-240 VAC)	252663-D72
	HP Modular Power Distribution Units (mPDU), High Volt Model, 40A (200-240 VAC)	252663-B21
	NOTE: This mPDU (252663-B21), 40A model has a hardwired input.	
	HP Modular Power Distribution Units (mPDU), High Volt Model, 16A (200-240 VAC)	252663-B24
	NOTE: This PDU has a detachable input power cord and allows for adaptability to country specific power requirements. This model may also be used with the high volt UPSs R3000 XR and R6000. Order cable PN 340653-001.	
	NOTE: Please see the following Modular Power Distribution Unit (Zero-U/1U Modular PDUs) QuickSpecs for additional options including shorter jumper cables and country specific power cords: http://www5.compaq.com/products/quickspecs/11041_na/11041_na.HTML	
PDU Options	Third Party Modular PDU Modular Kit NOTE: This kit allows you to mount the Modular PDUs in (1U configuration only) in racks other than the 9000/10000 Series racks (any racks using the standard 19" rail, including the 7000 Series racks). For more details please refer the Modular PDU QuickSpecs.	310777-B21
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (1 per pack)	142257-006
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (15 per pack)	142257-007
USB Options	USB Easy Access Keyboard (carbon)	267146-008
	USB Easy Access Keyboard (carbonite)	DC168B#ABA
	USB 2-Button Scroll Mouse (carbon)	195255-B25
	USB 2-Button Scroll Mouse (carbonite)	DC172B
	USB Floppy	304707-B21
Other	Enhanced Keyboard (Carbon)	296435-005
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (HD68)	159547-B22
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (VHDCI) NOTE: The ProLiant ML330/ML350 Internal to External SCSI Cable Option Kits (PN 159547-B21 and 333370-B21) are supported by the ML330/ML350 Family.	333370-B21
Rack Builder	Please see the Rack Builder for configuration assistance at http://www.compaq.com/rackbuilder/	
Rack Conversion Kit	ProLiant ML350 Generation 3 Tower to Rack Conversion Kit (CPQ branded)	290683-B21

HP Rack 10000 Series (Graphite Metallic)	HP S10614 (14U) Rack Cabinet - Shock Pallet	292302-B22
	HP 10842 (42U) Rack Cabinet - Pallet	257415-B21
	HP 10842 (42U) Rack Cabinet - Shock Pallet	257415-B22
	HP 10647 (47U) – Pallet	245160-B21
	HP 10647 (47U) – Crated	245160-B23
	HP 10642 (42U) – Pallet	245161-B21
	HP 10642 (42U) – Shock Pallet	245161-B22
	HP 10642 (42U) – Crated	245161-B23
	HP 10636 (36U) – Pallet	245162-B21
	HP 10636 (36U) – Shock Pallet	245162-B22
	HP 10636 (36U) – Crated	245162-B23
	HP 10622 (22U) – Pallet	245163-B21
	HP 10622 (22U) – Shock Pallet	245163-B22
	HP 10622 (22U) – Crated	245163-B23

NOTE: -B21 (pallet) used to ship empty racks shipped on a truck
-B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels)
-B23 (crated) used for air shipments of empty racks

NOTE: It is mandatory to use a shock pallet in order to ship racks with equipment installed. Not all Compaq equipment is qualified to be shipped in the Rack 10000 series.

NOTE: Please see the Rack 10000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color:
http://www5.compaq.com/products/quickspecs/10995_na/10995_na.HTML

NOTE: For additional information regarding Rack Cabinets, please see the following URL:
http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html
NOTE: This Web site is available in English only.

Compaq Rack 9000 Series (opal)	Compaq Rack 9142 (42U) – Pallet	120663-B21
	Compaq Rack 9142 (42U) – Shock Pallet	120663-B22
	Compaq Rack 9142 (42U) – Crated	120663-B23

NOTE: –B21 (pallet) used to ship empty racks shipped on a truck
–B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels)
–B23 (crated) used for air shipments of empty racks

NOTE: Please see the Rack 9000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color:
http://www5.compaq.com/products/quickspecs/10366_na/10366_na.HTML

NOTE: For additional information regarding Rack Cabinets, please see the following URL:
http://h18000.www1.hp.com/products/servers/proliantstorage/rack-ptions/index.html
NOTE: This Web site is available in English only.

Rack Options for HP Rack 10000 Series	Rack Blanking Panels – Graphite (Multi)	253214-B26
	NOTE: Contains one each of 1U, 2U, 4U and 8U.	
	Rack Blanking Panels – Graphite (1U)	253214-B21
	NOTE: The Rack Blanking Panels (PN 253214-B21) contains 10 each of (1U).	
	Rack Blanking Panels – Graphite (2U)	253214-B22
	NOTE: The Rack Blanking Panels (PN 253214-B22) contains 10 each of (2U).	
	Rack Blanking Panels – Graphite (3U)	253214-B23
	NOTE: The Rack Blanking Panels (PN 253214-B23) contains 10 each of (3U).	
	Rack Blanking Panels – Graphite (4U)	253214-B24
	NOTE: The Rack Blanking Panels (PN 253214-B24) contains 10 each of (4U).	
	Rack Blanking Panels – Graphite (5U)	253214-B25
	NOTE: The Rack Blanking Panels (PN 253214-B25) contains 10 each of (5U).	
	600mm Stabilizer Kit – Graphite	246107-B21
	800mm Wide Stabilizer Kit (Graphite)	255488-B21
	NOTE: Supported by the Rack 10842 cabinet only.	
	Baying Kit for Rack 10000 series (Carbon)	248[illegible]21
	42U Side Panel – Graphite Metallic	246099-B21
	110V Fan Kit (Graphite)	257413-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 5-15P.	
	220V Fan Kit (Graphite)	257414-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 6-15P.	
	36U Side Panel – Graphite Metallic	246102-B21
	47U Side Panel – Graphite Metallic	255486-B21
	9000/10000 Series Offset Baying Kit (42U)	248931-B21
	NOTE: This kit can be used to connect 9000 and 10000 series racks of the same U height together. Kit contents include hardware for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	
	NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-ptions/index.html NOTE: This Web site is available in English only.	

Options

Rack Options for Compaq Rack 9000 Series	Baying/Coupling Kit	120669-B21
	42U Side Panel	120670-B21
	NOTE: The 42U Side Panel (PN 120670-B21) supports the Compaq Rack 9142 and Compaq Rack 9842.	
	36U Side Panel	120671-B21
	NOTE: The 36U Side Panel (PN 120671-B21) supports the Compaq Rack 9136.	
	600mm Stabilizer Option Kit	120673-B21
	800mm Stabilizer Option Kit (Opal)	234493-B21
	NOTE: The 800mm Stabilizer Kit (PN 234493-B21) supports the Rack 9842 only.	
	9142 Extension Kit	120679-B21
	NOTE: The 9142 Extension Kit (PN 120679-B21) supports the Compaq Rack 9142 only.	
	Stabilizer Option Kit	120673-B21
	Rack Blanking Panel Kit for Rack 9000 series (Opal) (U.S.) NOTE: The Rack Blanking Panel Kit (PN 169940-B21) contains 4 panels – one each of 1U, 2U, 4U and 8U.	169940-B21
	Rack Blanking Panels (1U) NOTE: The Rack Blanking Panels (PN 189453-B21) contains 10 each of (1U).	189453-B21
	Rack Blanking Panels (2U) NOTE: The Rack Blanking Panels (PN 189453-B22) contains 10 each of (2U).	189453-B22
	Rack Blanking Panels (3U) NOTE: The Rack Blanking Panels (PN 189453-B23) contains 10 each of (3U).	189453-B23
	Rack Blanking Panels (4U) NOTE: The Rack Blanking Panels (PN 189453-B24) contains 10 each of (4U).	189453-B24
	Rack Blanking Panels (5U) NOTE: The Rack Blanking Panels (PN 189453-B25) contains 10 each of (5U)	189453-B25
	9136 Extension Kit	218216-B21
	9142 Short Rear Door NOTE: The 9142 Short Rear Door (PN 218217-B21) supports the Compaq Rack 9142 only.	218217-B21
	Split Rear Door (Opal) NOTE: The Split Rear Door (PN 254045-B21) supports the 600 mm wide, 42U 9000 series rack.	254045-B21
	9136 Short Rear Door	218218-B21
	9142 Split Rear Door	254045-B21
	9000/10000 Offset Baying Kit (42U) NOTE: This kit can be used to connect 9000 and 10000 series racks of same U height together. Kit contents include hardware for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	248931-B21
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	
Rack Options for Compaq Rack 7000 Series	High Air Flow Rack Door Insert for the 7122 Rack	157847-B21
	High Air Flow Rack Door Insert for the 7142 Rack (single)	327281-B21
	High Air Flow Rack Door Insert for the 7142 Rack (6-pack)	327281-B22
	Compaq Networking Cable Management Kit	292407-B21
	Compaq Rack Extension Kit for 7142	154392-B21
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	

Options

Rack Options for Rack 7000, 9000 and 10000 Series	Monitor Utility Shelf	303606-B21
	Ballast Option Kit	120672-B21
	100kg Sliding Shelf	234672-B21
	Rack Rail Adapter Kit (25-inch depth)	120675-B21
	Cable Management D-Rings Kit	168233-B21
	Console Management Controller (CMC) Option Kit	203039-B21
	Console Management Controller (CMC) Sensors Option Kit	203039-B22
	Console Management Controller (CMC) Locking Option Kit	203039-B23
	Console Management Controller (CMC) Smoke Sensors Option Kit	203039-B24
	Server Console Switch 1 x 2 port (100 to 230 VAC)	120206-001
	Server Console Switch 1 x 4 port (100 to 230 VAC)	400336-001
	Server Console Switch 1 x 8 port (100 to 230 VAC)	400337-001
	Server Console Switch 2 x 8 port (100 to 230 VAC)	400338-001
	Server Console Switch 2 x 8 port (48 VDC)	400542-B21
	IP Console Switch Box, 1x1x16	262585-B21
	IP Console Switch Box, 3x1x16	262586-B21
	IP Console Interface Adapter, 8 pack	262587-B21
	IP Console Interface Adapter, 1 pack	262588-B21
	IP Console Expansion Module	262589-B21
	KVM 9 PIN Adapter (4 Pack)	149361-B21
	CPU to Server Console Cable, 12'	110936-B21
	CPU to Server Console Cable, 20'	110936-B22
	CPU to Server Console Cable, 40'	110936-B23
	CPU to Server Console Cable, 3'	110936-B24
	CPU to Server Console Cable, 7'	110936-B25
	CPU to Server Console Cable (Plenum Rated) 20'	149363-B21
	CPU to Server Console Cable (Plenum Rated) 40'	149364-B21
	IP CAT5 Cable 3', 4 pack	263474-B21
	IP CAT5 Cable 6', 8 pack	263474-B22
	IP CAT5 Cable 12', 8 pack	263474-B23
	IP CAT5 Cable 20', 4 pack	263474-B24
	IP CAT5 Cable 40', 1 pack	263474-B25
	Switch Box Connector Kit (115 V)	144007-001
	Switch Box Connector Kit (230 V)	144007-002
	1U Rack Keyboard & Drawer (Carbon)	257054-001
	NOTE: The 1U Rack Keyboard & Drawer (PN 257054-001) is to be used with the Keyboards for Racks with Trackball (PN 158649-001).	
	TFT5600 Rack Keyboard Monitor	221546-001
	Input Device Adjustable Rails	287139-B21
	NOTE: Input Device Adjustable Rails (287139-B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	
	Input Device Telco Rail	287138-B21
	NOTE: Input Device Telco Rails (287138-B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	
	Keyboard/Monitor/Mouse extension cables	169989-001
	NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html	
	NOTE: This Web site is available in English only.	

HP Factory Express

Factory Installation, Racking, and Customization Services

Factory Express Server Configuration Level 1	293355-888

NOTE: Free Installation of HP Options - Installation of HP Options memory, NICs, hard drives, controllers, processors, I/O cards, pre-install standard OEM OS image, and tape drives. Installation fees will apply to all non-HP certified hardware and asset tags.
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Factory Express Server Configuration Level 2	266326-888

NOTE: Includes Level 1 Customer Intent of a ProLiant server and options configuration, OS installation, custom image download, IP addressing, network setting, and custom packaging. Customer unique requirements (quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, and RILOE). Customer access, validation and control through VPN (price/server).
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Factory Express Rack Integration Level 3 with 1 - 3 servers or storage enclosures	325736-888
Factory Express Rack Integration Level 3 with 4 - 9 servers or storage enclosures	232539-888
Factory Express Rack Integration Level 3 with 10 or more servers or storage enclosures	325735-888

NOTE: Includes Level 1 Customer Intent for standard mounted servers and storage units plus standard cable mgmt, RAID configuration, servers & storage, power distribution, networking gear and accessories (price/ra520ck).
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Factory Express Rack Integration Level 4 with 1 - 3 servers or storage enclosures	325734-888
Factory Express Rack Integration Level 4 with 4 - 9 servers or storage enclosures	232540-888
Factory Express Rack Integration Level 4 with 10 or more servers or storage enclosures	325733-888

NOTE: Includes Level 2 Customer Intent plus customer defined cable management and naming convention, customer furnished image download, IP addressing, cluster configurations (SQL, External storage RAID). Quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, RILOE). Customer access and validation through VPN (price/rack).
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Factory Express Rack Integration Level 5 with 1 - 3 servers or storage enclosures	325732-888
Factory Express Rack Integration Level 5 with 4 - 9 servers or storage enclosures	232541-888
Factory Express Rack Integration Level 5 with 10 or more servers or storage enclosures	325731-888

NOTE: Includes Level 4 Customer Intent plus Custom SW layering and extended test, Customer access, validation and control through VPN, Clustered racks with networking gear and/or external storage array, Start-up installation services custom quote. (price/rack).
NOTE: Factory Express Engineered Solution Level 6 is a custom solutions available through Factory Express. Please contact a your local reseller or Account Manager.
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Service and Support Offerings (HP Care Pack Services)

Hardware Services On-site Service

4-Hour On-site Service, 5-Day x 13-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL3EC-36
4-Hour On-site Service, 5-Day x 13-Hour, 3 Years (U.S. Part Number)	331045-002
4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL7EC-36
4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	162675-002
6-Hour Call to Repair, On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-ELCEC-36
6-Hour Call to Repair, On-site Service 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	331046-002

6.156

Options

Installation & Start-up Services

Hardware Installation (Canadian Part Number)	FP-ELINS-EC
Hardware Installation (U.S. Part Number)	401791-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	240013-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on o scheduled bosis 8am-5pm, M-F, excl. HP holidays. (Canadian Part Number)	FM-MSTEC-01
Installation & Start-Up of a ProLiont server and Linux O/S per the Customer Description and/or Dota Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	331051-002
Installotion & Start-Up of a ProLiant server ond Linux O/S per the Customer Description and/or Dato Sheet. To be delivered on a scheduled bosis 8am-5pm, M-F, excl. HP holidoys. (Canodian Part Number)	FM-LSTEC-01

Support Plus

Onsite HW support, 8am-9pm, M-F, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Port Number)	2399[illegible]002
Onsite HW support, 8am-9pm, M-F, 4hr response ond Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8om-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-M01E1-36
Onsite HW support, 8am-9pm, M-F, 4hr response ond Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidoys. (U.S. Part Number)	331049-002
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-L01E1-36

Support Plus 24

Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number)	239930-002
Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canodian Port Number	FM-M02E1-36
Onsite HW support 24x7, 4hr response ond Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number	331050-002
Onsite HW support 24x7, 4hr response ond Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canodian Part Number	FM-L02E1-36

CarePaq Priority Services for ProLiant Servers – Priority Silver

24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Manager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (2-5-2 Part Number for Canada)	FM-M04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (2-5-2 Part Number for Canada)	FM-M24E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (2-5-2 Part Number for Canada)	FM-N04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (2-5-2 Part Number for Canada)	FM-N24E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Manager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (6-3 Part Number for U.S.)	239932-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (6-3 Part Number for U.S.)	239934-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (6-3 Part Number for U.S.)	239972-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (6-3 Part Number for U.S.)	239974-002

NOTE: For more information, customer/resellers can contact http://www.hp.com/services/carepack

6-154

HP ProLiant ML350 G3 Array Models

The ML350 G3 supports both interleaved and non-interleaved memory configurations. Array models ship standard with one 512MB DIMM, non-interleaved. For best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory and installing in pairs is not required. Add any combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory

512MB (expandable to 8GB) of 2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models, with Advanced ECC capabilities (1x 512MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect and correct single bit memory errors while Advanced ECC extends this coverage to include protection against multiple simultaneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within a single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standard Memory Plus Optional Memory

Up to 6.7 GB of total memory can be implemented with the installation of three optional PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory

Up to 8.2 GB of total memory can be implemented with the removal of the standard 512-MB DIMM and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

NOTE: Charts do not represent all possible memory configurations.

		Slot 1	Slot 2	Slot 3	Slot 4
Standard	512 MB	512 MB	Empty	Empty	Empty
Optional	6656 MB	512 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB
2x1 Interleaved Memory (Recommended)		Pair 1		Pair 2	
	Total Memory	Slot 1	Slot 2	Slot 3	Slot 4
Recommended Configurations for Array Models	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

Following are memory options available from HP:

● 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
● 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21
● 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21

NOTE: To invoke interleaving in your array model, order this kit for a total of 1-GB of interleaved memory.

● 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
● 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21

Memory

HP ProLiant ML350 G3 Non-Array Models
The ML350 G3 supports both interleaved and non-interleaved memory configurations. Base models ship standard with one 256MB DIMM, non-interleaved. For best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory and installing in pairs is not required. Add any combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory
256MB (expandable to 8GB) of 2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advanced ECC capabilities (1x 256MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect and correct single bit memory errors while Advanced ECC extends this coverage to include protection against multiple simultaneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within a single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standard Memory Plus Optional Memory
Up to 6.4 GB optional memory is available with the installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory
Up to 8.2 GB of memory is available with the removal of the standard 256-MB of memory and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMM installed.

NOTE: Charts do not represent all possible memory configurations

Memory					
		Slot 1	Slot 2	Slot 3	Slot 4
Standard	256 MB	256 MB	Empty	Empty	Empty
Optional	6400 MB	256 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB

Recommended Configurations for Base Models	Total Memory Desired	1	2	3	4
	512 MB	256 MB	256 MB	Empty	Empty
	1 GB	256 MB	256 MB	256 MB	256 MB
	1.5 GB	256 MB	256 MB	512 MB	512 MB

Recommended Configurations for Array models	Total Memory Desired	1	2	3	4
	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

Following are memory options available from HP:

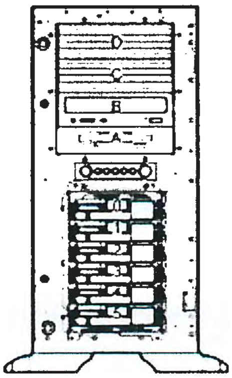
- 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB) 287494-B21
- 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB) 287495-B21

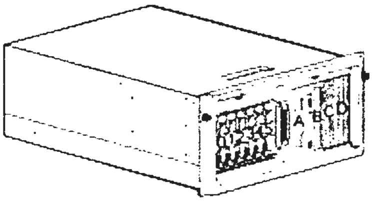
NOTE: To invoke interleaving in your base model, order this kit for a total of 512MB of interleaved memory.

- 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB) 287496-B21
- 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB) 287497-B21
- 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB) 301044-B21

6.152

Storage





0 - 5	6 x 1 in SCSI Hard Drive Bays
A	3.5 in Diskette Drive
B	48x CD-ROM
C, D	Available half height bay

Drive Support

	Quantity Supported	Position Supported	Controller
Removable Media			
1.44-MB Diskette Drive	Up to 1	A	Integrated
IDE (ATAPI) CD-ROM Drive	Up to 2	B, C, D	Integrated IDE (ATAPI)
DVD-ROM Drive Option Kit	Up to 2	B, C, D	Integrated IDE
ML3xx Two Bay Hot Plug SCSI Drive Cage	Up to 1	C, D	Integrated SCSI

Storage

Hard Drives

Ultra320 Hot Pluggable Drives

	Quantity Supported	Position Supported	Controller
1-inch 146.8-GB 10,000 rpm 72.8-GB 10,000 rpm 36.4-GB 10,000 rpm 72.8-GB 15,000 rpm 36.4-GB 15,000 rpm 18.2-GB 15,000 rpm	Up to 6	0-5	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

NOTE: All U320 Universal Hard Drives are backward compatible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates.

Wide Ultra320 SCSI – Non-Hot Plug

	Quantity Supported	Position Supported	Controller
1-inch 36-GB 10,000 rpm	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

External Storage

	Quantity Supported	Position Supported	Controller
StorageWorks Enclosure 4300 Family (supports Ultra3/Ultra320 1" drives)	Up to 24	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
3U Rackmount Kit 5U Rackmount Kit	Up to 3	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
MSA 1000	Please see the MSA 1000 QuickSpecs below to determine configuration requirements	External	Please see the MSA 1000 QuickSpecs (URL below) for the latest list of supported HBAs

MSA 1000: http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML

Maximum Storage Capacity – (StorageWorks Enclosure)

Internal	1.174 TB (6 x 146.8-GB 1" Ultra320 hot plug hard drives with standard internal drive cage + 2 x 72.8-GB 1^{2}"Ultra320 Hot plug hard drive using the optional ML3xx Two Bay Hot Plug SCSI Drive Cage)
External	49.324 TB (14 x 146.8 GB) x 24
Total	50.498 TB

Tape Drives

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Drives listed below, please see the following: http://www5.compaq.com/products/quickspecs/North_America/10233.html

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Storage Systems listed below, please see the following: http://www5.compaq.com/products/quickspecs/North_America/10809.html

	Quantity Supported	Position Supported	Controller
Internal AIT 100-GB, Hot Plug Internal AIT 50-GB, Hot Plug Internal AIT 35-GB, LVD Hot Plug Internal 20/40-GB DAT Drive, Hot Plug Internal DAT 72, Hot Plug *Installation of AIT/DAT hot plug drives in D+C requires the optional Two Bay Hot Plug SCSI Drive Cage (PN 244059-B21)	Up to 3	0+ 1, 2+ 3, D+ C*	Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter *NOTE: The Smart Array 532 Controller does not support the AIT 100-GB Hot Plug Tape Drive.
20/40-GB DAT DDS-4 Tape Drive Internal 12/24-GB DAT Drive Internal DAT 72	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 35GB, Autoloader	Up to 4	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT Enhanced	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT VS	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB Internal AIT 50-GB Internal AIT 35-GB, LVD Internal	Up to 2	C, D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 230, Internal LTO Ultrium 460, Internal	Up to 1	C + D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SDLT 110/220-GB, Internal SDLT 160/320-GB, Internal	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External DAT 72	2	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB External AIT 50-GB External AIT 35-GB, LVD External	2	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External 40/80-GB DLT Enhanced External 40/80-GB DLT VS External 20/40-GB DLT	Up to 3	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 215, External LTO Ultrium 230, External LTO Ultrium 460, External	Up to 2	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

SDLT 110/220-GB, External SDLT 160/320-GB, External	Up to 2	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
20/40-GB DAT 8 Cassette Autoloader External	Up to 1	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SSL2020 AIT Library	2 drives per SCSI channel	External	SAN Access Module for Smart Array 5302 Controller
MSL5026DLX (40/80GB DLT-based) MSL5026SL (SDLT-based) Library MSL5052SL (SDLT-based) Library MSL5030L (LTO-based) Library MSL5060S (LTO-based) Library	2 drives per SCSI channel	External	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS

Power Specifications

Part Number	264166-001
Spare Kit	292237-001
Operational Input Voltage Range (V rms)	90 to 264
Frequency Range (Nominal) (Hz)	47 to 63 (50/60)

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Max Rated Output Wattage Rating	500	500	500	500	500	500
Nominal Input Current (A rms)	7.8	6.7	3.7	3.4	3.2	3.0
Max Rated Input Wattage Rating (Watts)	769	758	746	735	725	714
Max. Roted VA (Volt-Amp)	785	773	761	750	739	729
Efficiency (%)	65	66	67	68	68	70
Power Factor	0.98	0.98	0.98	0.98	0.98	0.98
Leakage Current (mA)	0.31	0.36	0.65	0.69	0.72	0.75
Maximum Inrush Current (A peak)	21	24	43	46	48	50
Maximum Inrush Current duration (miliseconds)	20	20	20	20	20	2[illegible]

System Specifications

ML350 Generation 3 (G3) Fully Configured

Up to 2 Processors, 4 Memory Slots, 8 Hard Drives, 5 PCI Slots, and 2 Hot Plug Power Supplies

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Fully Loaded System Input Wattage (W)	557	549	541	534	526	519
Fully Loaded System Input Current (A rms)	5.7	4.9	2.7	2.5	2.3	2.2
Fully Loaded System Thermal (BTU-Hr)	1900	1872	1846	1820	1794	1770
Fully Loaded System VA (Volt-Amp)	569	560	552	545	537	530
System Leakage with all power supplies looded (mA)	0.63	0.72	1.30	1.38	1.44	1.50
System Inrush Current with all power supplies loaded (A)	42	48	86	92	96	100
Power cord requirements	Nema 5-15P to IEC320-C13			Option no./Spare no: See Power Cord chart		
	IEC320-C13 to IEC320-C14			Option no./Spare no: 142257-001/142258-B21		

NOTES:

ActiveAnswers Power Calculotion

Power calculator is LIVE on ActiveAnswers Web site. This is on external link.

Follow this link: http://h30099.www3.hp.com/configurator/powercolcs.asp

NOTE: This Web site is available in English only.

To drill down to calculotors:

- Click on: "ProLiant Servers"
- Click on the Server of interest. Exomple: ML350 G3
- Click on: "Power Calculotor" link. (You moy need to scroll down to see it)

6.147
1

System Unit – Tower	Dimensions (HxWxD) (with feet/bezel)	18.5 x 10.25 x 26 in (46.99 x 26.04 x 66.04 cm)	
	Dimensions (HxWxD) (without feet/bezel)	17.5 x 8.5 x 24 in (44.50 x 21.59 x 60.96 cm)	
	Weight(approximate)	60 lb (27.24 kg) (without hard drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110 VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors	
		(Support for either two internal, two external, or o mix of internal/externol is ovoiloble. This is ochieved using on internol to externol SCSI coble option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Roted Steady-State Power	500W
	Temperature Range	Operoting	50° to 95° F (10° to 35° C) (No direct sustoining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

TechSpecs

System Unit – Rack	Dimensions (HxWxD)	8.61 x19 x 24 in (21.87 x48.26 x 60.96 cm)	
	Weight(approximate)	60 lb (27.24 kg) (without hard drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110 VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors (Support for either two internal, two external, or a mix of internal/external is available. This is achieved using an internal to external SCSI cable option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	500W
	Temperature Range	Operating	50° to 95° F (10° to 35° C) (No direct sustaining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

1.44-MB Diskette Drive	LED Indicators (front panel)	Green	
	Read/Write Capacity per Diskette (high/low density)	1.44 MB/720 KB	
	Drive Supported	One	
	Drive Height	One-third	
	Drive Rotation	300 rpm	
	Transfer Rate (high/low)	500 K/250 K bits/s	
	Bytes/Sector	512	
	Sectors/Track (high/low)	18/9	
	Tracks/Side (high/low)	80/80	
	Access Times	Track-to-Track (high/low)	3/6 ms
		Average (high/low)	169/94 ms
		Settling Time	15 ms
		Latency Average	100 ms
	Cylinders (high/low)	80/80	
	Read/Write Heads	Two	

TechSpecs

48X Max IDE (ATAPI) CD-ROM Drive	Disk	Applicable Disk	CD-ROM, CD-XA, CD-DA (Mode 1, Mode 2, Form 1 and 2) Photo CD (Single and Multi-session) Mixed Mode (Audio and Data combined) CD-R
		Capacity	540 MB (Mode 1, 12 cm) 650 MB (Mode 2, 12 cm)
	Block Size	Mode 1	2,048 bytes
		Mode 2	2,340 bytes, 2,336 bytes
		CD-DA	2,352 bytes
		CD-XA	2,328 bytes
	Interface	IDE (ATAPI)	
	Access Times (typical)	Random	<100 ms
		Full-Stroke	<150 ms
	Data Transfer Rate	Sustained	3000 to 7200 KB/s (20X to 48X)
		Burst	150 KBps to 7,200 KBps
		Bus Rate	16.7 MBps
	Cache Buffer	128 KB	
	Start-up Time (typical)	< 7seconds	
	Stop Time	< 4seconds	
	Laser Parameters	Type	Semiconductor Laser GaA1As
		Wave Length	780 ± 25 nm
	Operating Conditions	Temperature	41° to 113° F (5° to 45° C)
		Humidity	10% to 80%
	Dimensions	(HxWxD, maximum)	1.7 x 5.85 x 8.11 in (4.29 x 14.86 x 20.60 cm)
		Weight	2.09 lb (0.95 kg)

NC7760 PCI Gigabit Server Adapter (embedded)	Network Interface	10Base-T/100Base-TX/1000Base-TX	
	Compatibility	IEEE 802.3 10Base-T	
		IEEE 802.3ab 1000Base-T	
		IEEE 80.3u 100Base-TX	
	Data Transfer Method	32-bit bus-master PCI	
	Network Transfer Rate	10Base-T(Half-Duplex)	10 Mb/s
		10Base-T(Full-Duplex)	20 Mb/s
		100Base-TX(Half-Duplex)	100 Mb/s
		100Base-TX(Full-Duplex)	200 Mb/s
		1000Base-TX	1000Mb/s
	Connector	RJ-45	
	Cable Support	10Base-T	Categories 3, 4 or 5 UTP; up to 328 ft (100 m)
		10/100/1000Base-TX	Category 5 UTP; up to 328 ft (100 m)

Integrated Dual Channel Wide Ultra3 SCSI Adapter	Drives Supported	Up to 28 SCSI devices (14 per channel)
	Data Transfer Method	64-bit PCI bus-master
	SCSI Channel Transfer Rate	80 MB/s per channel
	Maximum Transfer Rate per PCI Bus (peak)	133 MB/s per channel
	SCSI Protocols	Wide Ultra2 SCSI Wide-Ultra SCSI-3 Fast SCSI-2
	Electrical Protocol	Low Voltage Differential (LVD)
	SCSI Termination	Active Termination
	External SCSI Connectors	Two 80-Pin VHDCI connectors
	Internal SCSI Connectors	Two 68-Pin Wide-Ultra SCSI-3 connectors

Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with the 2.8 GHz Array Models only)	Protocol	Ultra320 SCSI
	SCSI Electrical Interface	Low Voltage Differential (LVD)
	Drives Supported	Up to 6 Ultra 320, Ultra3 and Ultra2 SCSI hard drives
	SCSI Port Connectors SA-641	one internal SCSI port
	Data Transfer Method	64-Bit PCI bus-master
	PCI Bus Speed	64-bit, 133-MHz PCI-X (1 GB/s maximum bandwidth)
	PCI	3.3 volt PCI slot compatibility only
	Simultaneous Drive Transfer Channels	Two
	Channel Transfer Rate	320-MB/s total; 320-MB/s per channel
	Software upgradeable Firmware	Yes
	Cache Memory	64-MB DRAM used for code, transfer buffers, and non-battery backed read cache
	Logical Drives Supported	32
	Maximum Capacity	880.8 GB (6 X 146.8 GB)
	Memory Addressing	64-bit, supporting servers memory greater than 4 GB
	RAID Support	RAID 5 (Distributed Data Guarding) RAID 1+ 0 (Striping & Mirroring) RAID 1 (Mirroring) RAID 0 (Striping)
	Upgradeable Firmware	2-MB Flashable ROM
	Disk Drive and Enclosure Protocol Support	Ultra 320, Ultra2 and Ultra3
	Warranty	Maximum: The remaining warranty of the HP server product in which it is installed (to a maximum three-year limited warranty) Minimum: One-year, on-site limited warranty Pre-Failure Warranty: Drives attached to the Smart Array Controller and monitored under Insight Manager are supported by a Pre-Failure (replacement) Warranty. For complete details, consult the HP Support Center or refer to your HP Server Documentation.

TechSpecs

Video Controller	Controller Chip	ATI RAGE XL
	Video DRAM	8 MB Video SDRAM
	Data Transfer Method	32-bit PCI
	Support Resolution	Supported Color Depths:
	640 x 480	16.7M, 64K, 256, 16
	800 x 600	16.7M, 64K, 256, 16
	1024 x 768	16.7M, 64K, 256, 16
	1152 x 864	16.7M, 64K, 256, 16
	1280 x 1024	16.7M, 64K, 256, 16
	1600 x 1200	64K, 256, 16
	Connector	VGA

The information contained herein is subject to change without notice.

Microsoft and Windows NT are US registered trademarks of Microsoft Corporation. Intel is a US registered trademark of Intel Corporation.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Apêndice EM

GLOSSARY

A

Address book A record of people who can receive e-mail or pager notification as part of the enforcement of a security policy. The address book contains the names of the contacts as well as e-mail and pager addresses.

Agent The aspect of the Host Sensor system that is installed on each host in your network. An agent serves as a protective layer surrounding a computer's operating system kernel identifying and preventing suspected breaches of security and malicious attacks.

Agent Group A defined set of agents. Agent groups are created and modified from the **Agent Management** view of the Host Sensor system.

All Agents Group Default group to which all agents belong. Agents cannot be deleted from this group.

Attack An attempted breach of system security. Successful attacks range in severity from someone having an unauthorized view of data on your system to destroying or stealing data or shutting down your system.

B

Back orifice A remote administration tool that can provide unwanted access to and control of a computer by way of its Internet link. BO runs on Widows 95/98 and Windows NT.

Backbone In a LAN, the lines used to connect building to building, or to connect to a WAN. In a WAN, the set of paths to which local or regional networks connect.

Backdoor A planned security breach in an application that can allow unauthorized access to data.

Brute force A hacking method used to find passwords or encryption keys by trying every possible combination of characters until the code is broken.

Buffer overflow attack The method of overfilling a software buffer in order to insert and execute some other code with elevated privileges, often a shell from which further commands can be issued.

C

Camping out A hacking technique of breaking into a system and then finding a safe place from which to monitor the system, store information, or re-enter the system at some later time.

CERT Computer Emergency Response Team. Established in 1988 by the Defense Advanced Research Projects Agency, CERT is chartered to facilitate the Internet community's response to computer security events. www.cert.org.

Ciphertext An encrypted form of plaintext.

Console user Console users have full access to Host Sensor system functionality, with the exception of user management.

Console The GUI application that provides monitoring and management of the Host Sensor system.

D

DARPA Defense Advanced Research Projects Agency. Department of Defense agency responsible for the development of military technology. Funded much of the development of the Internet, including Berkeley UNIX and TCP/IP.

Database The repository of all data necessary to the valid operation of the Host Sensor system, as well as all data collected and reported by agents.

Datagram See packet.

Decryption The process of converting encrypted data back into its original form.

Denial of Service An attack method whereby a computer is overwhelmed with bogus requests, causing it to crash or keeping it from honoring legitimate requests.

DNS Domain Name System. A system on the Internet that maps host names to IP Addresses for the purpose of making network connections. DNS also makes the reverse map (IP Address to host name) for the purpose of authentication.

Domain installation The type of installation the Host Sensor system uses if you are operating under a Windows NT Domain architecture and want the Host Sensor server to retrieve user group information from the Primary Domain Controllers in your network.

E

Encryption The conversion of data from plaintext to ciphertext in order to keep the contents secure.

Event Recognition of a signature by an agent (security event); any of a defined set of Host Sensor system activities (system event).

Exception The mechanism for overriding security policies to minimize false positive alerts. Exceptions are defined for specific security events.

F

False positive A security event triggered by a benign process rather than an attack.

Finger A program that displays information about users logged on to a local or remote system.

Firewall A set of programs installed on a gateway server, designed to protect the resources of that network from users on other networks. A firewall filters and routes incoming traffic, and makes outgoing requests (to the Internet, for instance) on behalf of local workstations.

Fragmentation The IP process in which a packet is divided into smaller pieces (fragments) to pass over a network. The fragments are reassembled by the IP layer at the destination.

H

Host Any computer on the Internet that has full two-way access to other computers on the Internet.

Host-based security system A security application that functions by virtue of being installed on and protecting each node (host) in a network.

I

ICMP An extension to IP that allows for the generation of error messages and test packets.

IP address A 32-bit number that identifies each computer sending or receiving information via packets across the Internet. An IP Address has two parts: one identifying the network, the other identifying the specific server or workstation.

L

LAN Local Area Network. A network of servers, workstations and peripheral devices usually confined to a single building or other geographically limited area.

Local installation The type of installation the Host Sensor system uses if you are operating in a workgroup environment.

M

Mode The manner in which an agent has been set to protect its host. There are four possible modes for an agent: **On-Protecting, On-Warning, Off-Protecting, Off-Warning.**

N

Network A series of nodes connected by communication paths. Networks can interconnect with one another and contain subnetworks.

New Agents Group Agent group comprised of newly installed agents making their first contact with the server. Agents remain part of the **New Agents** group until they are removed manually.

Notification An alert dispatched by the Host Sensor system as defined in a security policy. There are four methods of notification: e-mail, pager, SNMP trap, spawned process.

NT registry A database that stores the configuration data of a computer operating under Windows NT. Stored data include attached hardware, system settings and programs to be started along with the operating system.

O

Off-Protecting Agent is deactivated and performs no security measures; the agent is in protection mode when it is reactivated.

Off -Warning Agent is deactivated and performs no security measures; the agent is in warning mode when it is reactivated.

On-Protecting Agent detects signatures, logs events and carries out all security measures.

On-Warning Agent detects signatures and logs events, but does not carry out security measures.

P

Packet A unit of data routed from an origin to a destination on the Internet. Any file sent from one place to another on the Internet is divided into packets by the TCP layer of TCP/IP at the point of origin. The TCP layer at the destination reassembles the packets into the original file.

Packet filter A part of a firewall, a packet filter examines incoming packets in order to permit or deny entry to the network.

Packet sniffer A sniffer on a TCP/IP network that examines the contents of all packets on that network. See **Sniffer.**

Packet switching A method of sending data through a network based on the destination address contained within each packet.

PGP Pretty Good Privacy. A technique for encrypting messages that uses the public key method. The pubic key is distributed to those from whom you wish to receive encrypted messages; the private key is held by you to decrypt messages. Developed by Philip Zimmerman; freely available from the Massachusetts Institute of Technology.

Ping Packet InterNet Groper. A program used to test whether a host is operating. Ping sends an ICMP echo request and waits for a reply.

Ping attack The method of overwhelming a network with ping commands.

Ping of death A hacking technique used to cause a denial of service by sending a large ICMP packet to a target. As the target is attempting to reassemble the packet, the size of the packet overflows the buffer and can cause the target to reboot or hang.

Plaintext Ordinary, readable text. Opposite of ciphertext.

Port scanning A hacking technique used to check TCP/IP ports to reveal what services are available in order to plan an exploit involving those services, and to determine the operating system of a particular computer.

Protection mode The mode in which an agent monitors activity on its host and carries out security measures.

Protocol A formal description of the set of rules and conventions that govern how devices on a network exchange information.

PSN Packet Switch Node. A dedicated computer used to accept, route and forward packets in a packet switched network.

publickey A file generated during installation of the Host Sensor system. This file must be copied to the Cisco HIDS Agent installation folder on each host, and is used by the agent to facilitate encrypted communication with the server.

Public key encryption A system of encrypting electronic files using a pair of keys: a public key used to encrypt a file, and a private key used to decrypt a file.

R

Reaction The response by an agent when intercepting a signature. There are four possible reactions: ignore the attack, log the attack in the database, prevent the specific illegal operation from taking place, and end the process that is performing the attack.

Remote login A terminal emulation program that allows a user to log on to a remote computer.

Router The path that network traffic follows from its origin to its destination.

S

Samba A program that implements the SMB protocol for UNIX systems, allowing UNIX and NT systems to share files and directories.

Security event The recognition of a signature by an agent.

Security level Definition of the danger implied by a signature. Signatures are given one of four security levels: **Info**, **Low**, **Medium**, and **High**.

Security policy The definition of reactions taken by agents when recognizing signatures, and the notifications that will be made in those cases.

Server An NT service that provides communication between agents and the database, and the database and the console.

Signature The description of a security threat or attack methodology.

Smurf attack A Denial of Service attack that floods its target with replies to ICMP echo (PING) requests. A smurf attack sends PING requests to internet broadcast addresses, which forward the PING requests to up to 255 hosts on a subnet. The return address of the PING request is spoofed to be the address of the attack target. All hosts receiving the PING requests reply to the attack target, flooding it with replies.

Sniffer An application that monitors and analyzes network traffic. Sniffers are used by network managers to detect problems with network traffic. They are also used by hackers to steal information. Sniffers are difficult to detect and can be inserted almost anywhere in a network (a primary reason for their popularity among hackers).

SNMP A network management protocol widely used in TCP/IP networks that provides the means to monitor and control network devices, as well as manage configuration, performance and security.

SNMP Trap A method of notification included in a security policy.

Snooping Passively observing a network.

Spawned process A method of notification included in a security policy. Any process that can be started from the Windows **Start>Run** menu can be used.

Spoofing Forging something, such as an IP Address to hide one's location and identity.

State Describes the manner in which an agent is actually functioning (Current State), or will be functioning after its next communication with the server (Requested State). The console recognizes six different states for an agent: On-Protecting, On-Warning, Off-Protecting, Off-Warning, Not connected, No license.

Stub network A network that carries packets to and from local hosts.

SYN flood A hacking technique used to cause a denial of service. SYN packets are sent from a client with a spoofed IP address and are sent at a rate faster than the TCP stack on the host is set to time out. As the client address is spoofed, the client sends no SYN-ACK, but continues to flood the host with SYN packets, tying up the resources of the host.

System All components of the Host Sensor.

System administrator This account has full access to Host Sensor system functionality including user management.

System event Any of a defined set of Host Sensor system activities.

T

TCP/IP Transmission Control Protocol/ Internet Protocol. The basic communication language of the Internet. The TCP layer divides outgoing data into packets and assembles incoming packets into the original file. The IP layer handles the address in each packet so that it arrives at the appropriate destination.

Telnet The user command and TCP/IP protocol for accessing a remote computer. Telnet allows you to log on to the remote computer as a user.

Testing group A specific agent group designated to receive a Test version of Host Sensor agent software.

TFN/Trinoo Tribal Flood Network. Distributed Denial of Service attacks based on TCP/IP architecture that use a large number of computers to simultaneously attack a target. The attack originates from a single computer controlling several master computers, which in turn each control a number of daemons (other compromised computers). The masters maintain a list of responding daemons, signaling them to initiate the attack. Trinoo floods the target with UDP packets. TFN uses SYN flood, UDP flood, ICMP flood or smurf attack.

Trojan horse Harmful or malicious code masked by apparently innocuous code. In addition to corrupting data or giving away passwords, a trojan horse can open a back door to a system, providing further unwanted access.

U

User group Any set of users defined on a Primary Domain Controller.

V

Version A release of Cisco IDS Host Sensor agent software. Any number of versions can be maintained on a server.

Version, Default A release of Host Sensor agent software that has been tested in the network environment and designated as Default. This version is distributed to all agents not in the testing group. There can be only one version designated as Default.

Version, New A release of Host Sensor agent software that is newer than the Default version.

Version, Old A release of Host Sensor agent software that is older than the Default version.

Version, Test A release of Host Sensor software designated as Test and distributed to a specific group of agents in order to check its functionality in a specific network environment. There can be only one version designated as Test.

W

WAN Wide Area Network. A data communications network that serves a broad geographic area.

Warning Mode The mode in which an agent can monitor activity on its host without carrying out security measures.

Worm A program that seeks to replicate itself from one computer to another, often damaging or stealing data in the process.

Apendice EN

CISCO SYSTEMS

Product Bulletin No. 1928

Cisco **Content Switching Module** Software Version 3.1(1) for the Cisco Catalyst 6500 Switch and the Cisco 7600 Internet Router

New Features

New features of the Cisco CSM Software Version 3.1(1) Content Switching Module for the Cisco Catalyst® 6500 Switch and the Cisco 7600 Internet Router include the following:

- *Virtual IP (VIP) connection watermarks*—The VIP connection watermark feature allows the Web-hosting provider to limit the number of connections going through a particular virtual server or set of virtual servers. By using this feature, the network administrator allows a fair distribution of connection resources among all virtual servers. When a virtual server reaches the configured maximum connection limit, no new connections are established to that virtual server until it drops below the connection watermark again. This feature allows Cisco CSM customers to have a shared CSM environment, whether between multiple customers or many departments with an enterprise, without fear that one group will consume all the resources. This feature also can be configured to protect against denial-of-service (DoS) attacks.
- *Backup server farm*—The backup server farm feature allows the administrator to specify one or more backup servers that will be used when all primary servers in a server farm are unavailable because of health probes or connection thresholds. If configured, when the Cisco CSM receives a connection that matches a policy associated with a server farm in which all the servers are currently down, the CSM load balances this connection to the configured backup server farm. The backup server farm also can be configured to be a Hypertext Transfer Protocol (HTTP) redirect so that clients are redirected to a remote location.
- *Optional port for health probing*—Some of the Cisco CSM supported health probes require that the CSM probe real servers on a specific TCP or User Datagram Protocol (UDP) port. In earlier implementations of Cisco CSM Software, the network administrator cannot explicitly specify a server port when configuring a health probe. Instead, the port is inherited from the virtual servers that are using the server farm with which the probe is associated. This feature allows the administrator to override the real and virtual server port information by explicitly specifying a port to probe in the health probe configuration.

- *IP reassembly*—In Cisco CSM 1.x Software releases, all IP fragments are dropped by the CSM. In Cisco CSM 2.x Software releases, the UDP fragments of a datagram are reassembled as long as the first fragment of the datagram is received by the Cisco CSM before all other fragments. In 3.1(1), the Cisco CSM can handle UDP fragments and assemble them, regardless of the order in which they were received.
- *Toolkit Command Language (TCL) scripting*—To support more flexible health-probing functionality, this feature gives the administrator the ability to upload and execute TCL scripts on the Cisco CSM. The administrator can create a "script probe" that the Cisco CSM periodically executes for each real server in any server farm associated with the probe. Depending upon the exit code of such a script, the real server is considered healthy, suspect, or failed. A wide variety of probing functions are possible using the flexibility of the TCL scripting environment. The Cisco CSM also supports execution of custom TCL scripts that are not directly associated with a particular server health probe. A "standalone script" dynamically executes a task at a specified interval.
- *Extended Markup Language application programming interface (XML API) configuration*—Users can now automate programmatic configuration of the Cisco CSM via a documented XML API. When the network administrator enables this feature, a network management device may connect to the CSM and "push" new configurations to it. The network management device pushes configuration commands to the Cisco CSM using the standard HTTP protocol by sending an XML document in the data portion of an HTTP POST. The full Document Type Definition (DTD) can be found documented in the appendix of the Cisco CSM Installation and Configuration Guide.
- *Simple Network Management Protocol/Management Information Base (SNMP/MIB)*—The Cisco CSM now has full SNMP/MIB support. In this release, the Cisco CSM supports two Read Only MIBs: CISCO-SLB-MIB and CISCO-SLB-EXT-MIB, which are available at ftp://ftp.cisco.com/pub/mibs/. Traps can be sent based on real server, virtual server, and fault tolerant state changes.
- *Global server load balancing (GSLB)*—GSLB has increased in popularity as a method for disaster recovery. In this release the Cisco CSM supports GSLB in which the CSM can be configured to act as an authoritative Domain Name System (DNS) server. The Cisco CSM then collects load information from other Cisco CSMs in the network and load balances incoming traffic across these geographically dispersed CSMs.
- *Resource usage display*—A show command has been added to the Cisco CSM that includes multiple parameters for determining how loaded the CSM is at a given moment. The output of this command indicates the CPU usage on each of the processing modules within the Cisco CSM hardware, memory usage, and other related information.
- *HTTP method parsing*—Every HTTP request contains an HTTP method, a URL, and other information such as HTTP headers. This new feature allows the user not only to match HTTP headers, but also to configure policies that match particular HTTP "methods," such as GET, HEAD, and POST, and to make a load-balancing decision based on this information.
- *Real server names*—The real server configuration on the Cisco CSM now includes assigning an ASCII string name in addition to the current options of IP address and port. This creates a friendlier way to reference real servers, mapping an IP address to a name. It also allows all instances of the real server to be removed from service on a global level with one command, regardless of how many server farms to which a real server belongs.
- *Non-TCP connection state redundancy*—The Cisco CSM currently supports connection state redundancy for TCP protocols. This functionality has been extended to include non-TCP protocols.

- *Reverse sticky*—In a firewall load-balancing environment, this feature allows multiple connections between the same two devices to be stuck to the same firewall based on the IP addresses of the first incoming connection, regardless of the load-balancing algorithm used and regardless of which of the two devices originated the connection. This feature is especially important for firewall load-balancing scenarios where the load balancers on the two sides of the "sandwich" are not both Cisco CSMs. As an example, when using Cisco IOS® SLB on one side of the sandwich and the Cisco CSM on the other, the hash algorithms are not the same; therefore, new connections originated by the receiving device might not be load balanced to the same firewall from which the first connection was received. With the Cisco CSM reverse sticky feature configured, the receiving Cisco CSM sets up a sticky entry for connections opened in the opposite direction. This way, after the first connection between two specific devices has been set up on the two Cisco CSMs in the firewall load-balancing sandwich, all subsequent connections are load balanced to the same firewall, regardless of which of the two devices originates them.
- *Unidirectional idle timeout*—This feature allows the user to configure unidirectional timers for specific virtual servers; for flows matching those virtual servers, the Cisco CSM monitors only one direction of the flow. This feature is particularly useful in UDP streaming environments, where unidirectional flows are common and long idle timers are not optimal; unidirectional timers for this kind of flows allow the Cisco CSM to ignore the silent direction of the flow and time out the flow based on only the other direction.
- *SSL service module ID*—The Cisco CSM now has a configurable sticky option that allows the CSM to continue to provide stickiness based on Secure Sockets Layer (SSL) ID, even during SSL ID renegotiation when the Cisco CSM is paired with the SSL Services Module for the Cisco Catalyst 6500. Though the renegotiation process is encrypted, usually making it impossible to use SSL ID effectively for stickiness, the Cisco CSM is able to work in conjunction with the Cisco SSL Services Module, when this feature is configured. This ensures that the stickiness is not broken, even if a SSL ID renegotiation occurs. The result is that the same SSL Service Module is always selected for the same client.

Orderable Product Numbers

Table 1 gives part numbers for ordering Cisco CSM Software.

Table 1 Cisco CSM Part Numbers

Cisco CSM Software Version	Hardware Part Number	Software Part Number	Hardware Requirements	Native Cisco IOS Software Release	Added Features
3.1(1)	WS-X6066-SLB-APC	SC6k-3.1.1-CSM	Supervisor IA with Multilayer Switch Feature Card (MSFC) and Policy Feature Card (PFC) or Supervisor II with MSFC 2	12.1(13)E	• VIP connection watermarks • Backup serverfarm • Optional port for probing • IP reassembly • Scriptable health checks • XML API for configuration • SNMP/MIB support • GSLB • Resource usage display • HTTP method parsing • Real server names • Non-TCP connection state redundancy • Reverse IP sticky • SSL services module ID • Unidirectional idle timeout
2.1(4)	WS-X6066-SLB-APC	SC6k-2.1.4-CSM	Supervisor IA with MSFC and PFC or Supervisor II with MSFC 2	12.1(8)EX	• Firewall load balancing • Non-TCP load balancing • URL hashing • HTTP 1.1 persistence • Full stateful failover • Generic header parsing • SNMP server health traps • Multiple Cisco CSMs in a chassis • Virtual private network/IP Security (VPN/IPSec) load balancing
2.2(4)	WS-X6066-SLB-APC	SC6k-2.2.4-CSM	Supervisor IA with MSFC and PFC or Supervisor II with MSFC 2	12.1(11)E	• Increased VLAN limit • Return code checking • Inband health monitoring • Configuration pending timeout value • Real-Time Streaming Protocol (RTSP) support

Further Information

Download the software release at:

http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-intellother

Cisco CSM Data Sheet:

http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/ccsm_ds.htm

Cisco CSM Installation and Configuration Guide:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/index.htm

Software Version 3.1(1) Release Notes:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_14716.htm

Marketing Contacts

Cisco CSM alias, ask-csm-pm@cisco.com

Dyan Gray, Product Manager, dpgray@cisco.com

Stefano Testa, Technical Marketing Engineer, testas@cisco.com

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: 65 317 7777
Fax: 65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

CISCO SYSTEMS

Data Sheet

Cisco Catalyst 6500 Series Switch

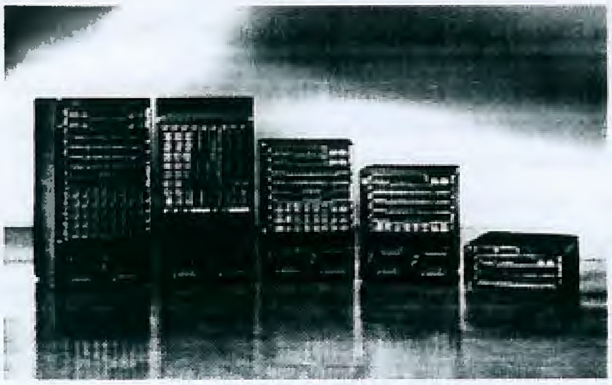
The Catalyst 6500 Series sets the new standard for IP communications and application delivery in enterprise campus and service provider networks by maximizing user productivity and enhancing operational control while providing unprecedented investment protection. As Cisco's premier intelligent multilayer modular switch, the Catalyst[®] 6500 Series delivers secure, converged services, end-to-end, from the wiring closet to the core, to the data center, to the WAN edge.

Ideal for enterprises and service providers seeking to reduce their total cost of ownership, the Cisco Catalyst 6500 Series delivers scalable performance and port density across a range of chassis configurations and LAN/WAN/MAN interfaces. Available in 3-, 6-, 9-, and 13-slot chassis, Cisco Catalyst 6500 Series switches feature an unparalleled range of integrated services modules, including multigigabit network security, content switching, telephony, and network analysis modules.

By taking advantage of a forward-thinking architecture that uses a common set of modules and operating system software across all Cisco Catalyst 6500 Series chassis, the Catalyst 6500 Series delivers a high level of operational consistency that optimizes IT infrastructure usage and enhances return on investment. From 48-port to 576-port 10/100/1000 Ethernet wiring closets to hundreds-of-Mpps network cores supporting up to 192 1-Gbps or 32 10-Gbps trunks, the Cisco Catalyst 6500 Series provides an optimal platform that maximizes network uptime with stateful failover capability between redundant routing and forwarding engines.

With numerous industry-firsts and industry-leading features to its credit, the Catalyst 6500 Series supports three generations of modules that continue to demonstrate the Catalyst 6500 value and Cisco's commitment to innovation. Cisco's new generation of Catalyst 6500 Series modules and Supervisor Engine 720 incorporate 11 new Cisco-developed application specific integrated circuits (ASICs)—extending Cisco's leadership in networking while providing unparalleled investment protection.

Figure 1
Cisco Catalyst 6500 Series Chassis



Cisco Catalyst 6500 Series Benefits

The Cisco Catalyst 6500 Series provides market-leading services, performance, port densities, and availability with investment protection for enterprise and service provider markets. These include:

- *Maximum network uptime*—With platform, power supply, supervisor engine, switch fabric, and integrated network services redundancy provides one- to three-second stateful failover and delivers application and services continuity in a converged network environment, minimizing disruption of mission-critical data and services
- *Comprehensive network security*—Integrates proven, multigigabit Cisco security solutions, including intrusion detection, firewall, VPN, and SSL into existing networks
- *Scalable performance*—Provides up to 400 Mpps performance with distributed forwarding architecture
- *Forward-Thinking architecture with investment protection*—Supports three generations of interchangeable, hot-swappable modules in the same chassis, optimizing IT infrastructure usage, maximizing return on investment, and reducing total cost of ownership
- *Operational consistency*—Features 3-, 6-, 9-, and 13-slot chassis configurations sharing a common set of modules, Cisco IOS Software, Cisco Catalyst Operating System Software, and network management tools that can be deployed anywhere in the network
- *Unparalleled services integration and flexibility*—Integrates advanced services such as security and content with converged networks, provides the widest range of interfaces and densities, from 10/100 and 10/100/1000 Ethernet to 10 Gigabit and from DS0 to OC-48, and performs in any deployment end to end

Operational Consistency in End-to-End Cisco Catalyst 6500 Series Deployments

- Features 3-, 6-, 9-, and 13-slot chassis configurations that share a common set of modules, software, and network management tools
- Deploys anywhere in the network—from the wiring closet to the core, to the data center, to the WAN edge
- Shares WAN port adapters with Cisco 7xxx router Series for reduced sparing and training costs
- Offers choice of Cisco IOS Software and Cisco Catalyst Operating System Software supported on all supervisor engines, providing smooth migration from Cisco Catalyst 5000 Series and Cisco 7500 Series deployments

Maximum Network Uptime and Network Resiliency

- Provides packet-loss protection and the fastest recovery from network disruption
- Features fast, one- to three-second stateful failover between redundant supervisor engines
- Offers optional, redundant high-performance Cisco Catalyst 6500 Series Supervisor Engine 720, passive backplane, multimodule Cisco EtherChannel® technology, IEEE 802.3ad link aggregation, IEEE 802.1s/w, Hot Standby Router Protocol/Virtual Router Redundancy Protocol (HSRP/VRRP) high-availability features

Integrated High-performance Security and Network Management

Integrated gigabit-per-second services modules, deployed where external devices would not be feasible, simplify network management and reduce total cost of ownership. These include:

- Gigabit firewall—provides access protection
- High-performance intrusion detection system (IDS)—provides intrusion detection protection
- Gigabit Network Analysis Module—provides a more manageable infrastructure and full Remote Monitoring (RMON) support
- High-performance SSL—provides high-performance, secure e-commerce traffic termination
- Gigabit VPN and standards-based IP Security (IPSec)—support lower cost Internet and intracampus connections

Content-and Application-Aware Layers 2 Through 7 Switching Services

- Integrated content switching module (CSM) brings high-performance, feature-rich server and firewall load balancing to the Cisco Catalyst 6500 Series, ensuring a safer and more manageable infrastructure with unprecedented control
- Integrated multigigabit SSL acceleration combined with CSM provides a high-performance e-commerce solution
- Integrated multigigabit firewall and CSM provide a secure, high-performance, data-center solution
- Software features such as Network Based Application Recognition (NBAR) enhance network management and control of bandwidth utilization

Scalable Performance

- Delivers the industry's highest LAN switch performance, 400 Mpps, using the distributed Cisco Express Forwarding dCEF720 platform
- Supports a mix of Cisco Express Forwarding (CEF) implementations and switch fabric speeds for optimal wiring closet, core, data center, and WAN edge deployments, as well as service provider networks

Rich Layer 3 Services

- Multiprotocol Layer 3 routing supports traditional network requirements and provides a smooth transition mechanism in the enterprise
- Provides hardware support for enterprise-class and service-provider-scale routing tables
- Provides IPv6 support in hardware (using Supervisor Engine 720) with an unparalleled high-performance suite of services
- Provides hardware support for large enterprise-class and service-provider-scale routing tables
- Provides MPLS support in hardware to enable VPN services within the enterprise and facilitate smooth integration with new high-speed service provider core infrastructures and Metro Ethernet deployments

Enhanced Data Voice, and Video Services

- Provides integrated IP communications throughout all Cisco Catalyst 6500 Series platforms
- Provides 10/100 and 10/100/1000 line cards, field upgradable with inline power using a daughter card and offering future support for IEEE 802.3af to protect today's investments
- Provides dense T1/E1 and foreign Exchange Station (FXS) voice-over-IP (VoIP) gateway interfaces for public switched telephone network (PSTN) access and traditional phone, fax, and private branch exchange (PBX) connections
- Supports high-performance IP multicast video and audio applications
- Provides integrated management necessary to effectively deploy a scalable enterprise-converged network

Highest Level of Interface Flexibility, Scalability, and Density

- Provides the port densities and interface choices that large mission-critical wiring closets, enterprise core, and distribution networks require
- Supports up to 576 voice 10/100/1000 Gigabit-over-copper ports with inline power per system
- Provides up to 192 Gigabit Ethernet ports

16.126
L

- Features the industry's first 10 Gigabit Ethernet, Channelized OC-48 dense OC-3 Packet over Synchronous Optical Network (SONET) (PoS)
- Provides investment protection by using Cisco 7xxx Series port adapters on the Cisco Catalyst 6500 Series FlexWAN Line Card, supporting T1/E1 through OC-48 WAN interfaces
- Chassis sizes range from 3-slot (Cisco Catalyst 6503 Switch) to 13-slot (Cisco Catalyst 6513 Switch)

High-Speed WAN Interfaces

- Provides high-speed WAN, ATM, and SONET interfaces compatible with other core routers
- Provides single-device management for WAN aggregation and for campus and metro connectivity

Maximum Investment Protection

- Highly flexible modular architecture supports multiple generations of modules that are fully interoperable with each other in the same chassis
- Upgradable supervisor engines can add Layer 3 routing or forwarding capabilities over time
- Cisco IOS Software and Cisco Catalyst Operating System Software are supported across all supervisor eng
- Field-upgradable inline power for 10/100 Mbps and 10/100/1000 Mbps Ethernet modules for "pay as you go" IP telephony and wireless computing
- A steady stream of new services modules adds to the deployment options
- Includes Cisco Catalyst 6500 Series network security, content switching, and voice capabilities
- Future modules will increase performance, port density, and include additional services

Ideal for Metro Ethernet WAN Services

- 802.1Q and 802.1Q tunneling (QinQ) providing point-to-point and multipoint Ethernet services
- EoMPLS in MPLS backbones for superior network scaling providing virtual LAN (VLAN) translation capability
- Layer 2 and Layer 3 QoS enables tiered Ethernet service offerings through rate limiting and traffic shaping
- Superior high-availability features include enhanced Spanning Tree Protocol, IEEE 802.1s, IEEE 802.1w, and Cisco EtherChannel IEEE 802.3ad link aggregation

Table 1 Catalyst 6500 Series at a Glance

Feature	Catalyst 6500 Series
System Feature	
Chassis Configurations	3-slot 6-slot 9-slot 9 vertical slots 13-slot
Backplane Bandwidth	32Gbps shared bus 256Gbps switch fabric 720Gbps switch fabric
L3 Forwarding Performance	Supervisor 1 MSFC: 15 Mpps Supervisor 2 MSFC: up to 210 Mpps Supervisor 720: up to 400 Mpps

Table 1 Catalyst 6500 Series at a Glance

Feature	Catalyst 6500 Series
Operating System	Catalyst OS (CatOS) Cisco IOS CatOS/IOS Hybrid Configuration
Redundant Supervisors	Yes, with stateful failover
Redundant Components	Power supplies (1+1) Switch fabric (1+1) Replaceable clock Replaceable fan tray
High Availability Features	Gateway Load Balancing Protocol Hot Standby Router Protocol Multimodule EtherChannel Rapid Spanning Tree Multiple Spanning Tree Per VLAN Rapid Spanning Tree Rapid Convergence L3 Protocols
Maximum System Port Densities	
10/100/1000 Ethernet	576 ports, all support Inline Power
10/100 Fast Ethernet	576 ports, all support Inline Power
100-Base-FX	288 ports
Gigabit Ethernet (GBIC)	194 ports (2 ports provided on supervisor engine)
10 Gigabit Ethernet (XENPAK)	32 ports
Integrated WAN Modules	
FlexWAN (DS0 to OC-3)	12 modules with 24 port adapters
OC-3 POS ports	192
OC-12 POS ports	48
OC-12 ATM ports	24
OC-48 POS/DPT ports	24
PSTN Interfaces	
Digital T1/E1 Trunk ports	216
FXS Interfaces	864
Advanced Services Modules	Gigabit Firewall Gigabit VPN High Performance Intrusion Detection Gigabit Content Switching Module High Performance SSL Termination Gigabit Content Services Gateway

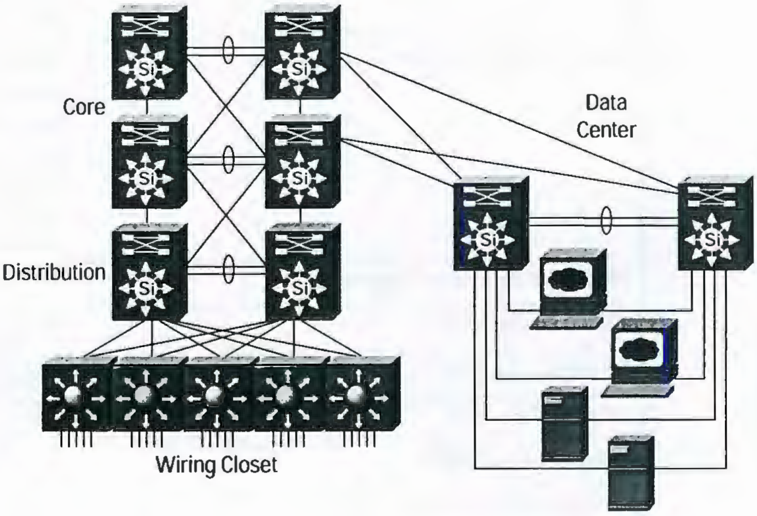
Deployment Scenarios

The Cisco Catalyst 6500 Series delivers secure converged services for campus, Internet service provider (ISP), metro edge, and research and grid computing networks.

- *Campus networks*—Features 10/100 and 10/100/1000 autosensing modules that provide inline power for the wiring closet, along with robust high availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the distribution and core

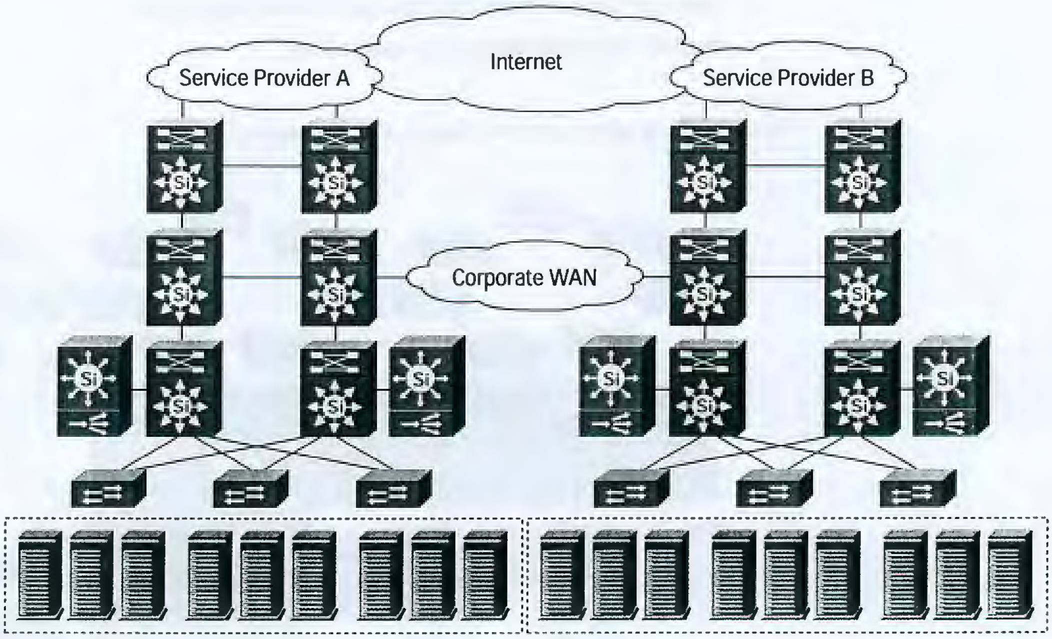
Figure 2

Deployment Scenarios for Catalyst 6500 Series Switches in Campus Networks



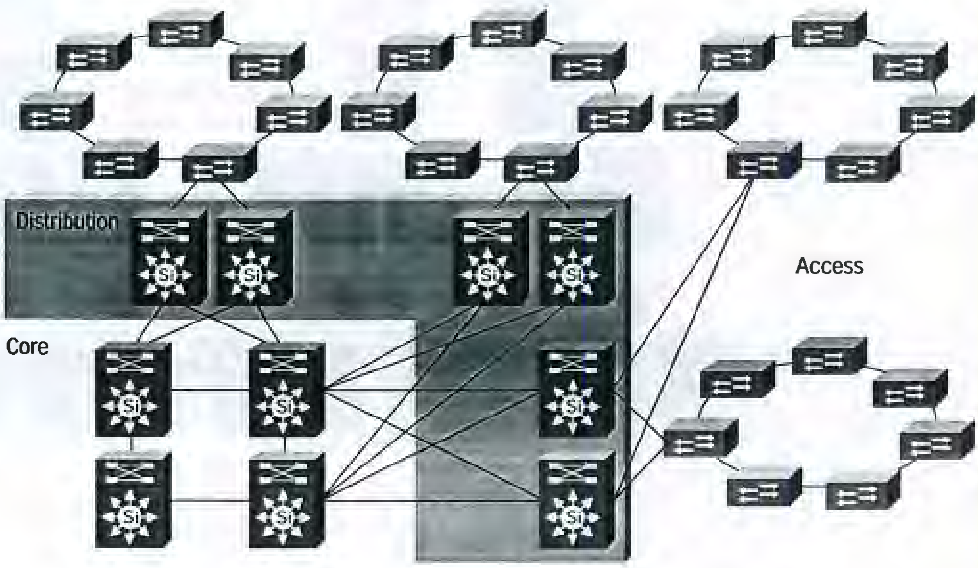
- [*ISP network*—Provides robust high-availability, security, and manageability features; world-class networking software; high-performance Gigabit and 10 Gigabit interface modules; and network management for the most demanding service provider networking environments requiring Multiprotocol Label Switching (MPLS), Multicast, IP Version 6 (IPv6), an extensive set of WAN interfaces, and hierarchical traffic shaping.

Figure 3
Deployment Scenarios for Catalyst 6500 Series Switches in ISP Networks



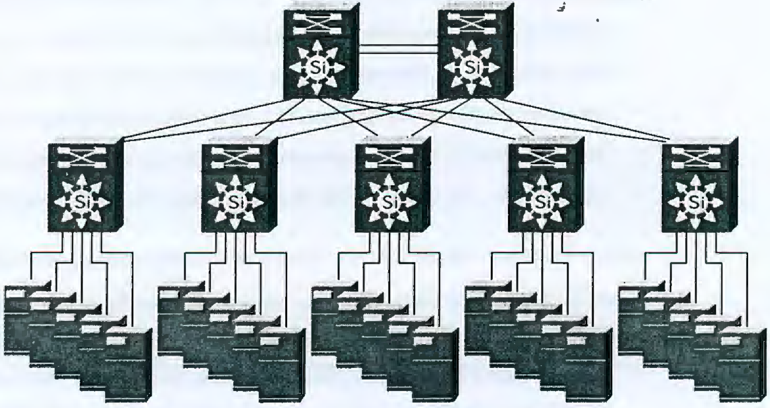
- *Metro edge*—Features edge-, distribution-, and core-layer interfaces for point-to-point and multipoint Ethernet services for metro and inter-metro network deployments with the following features:
  - High-performance 10-Gigabit Ethernet uplinks
  - 802.1Q tunneling
  - Ethernet over MPLS (EoMPLS)
  - Layer 2 and Layer 3 QoS
  - Network Equipment Building Standards (NEBS) compliance
  - Security, high availability, and manageability

Figure 4
Deployment Scenarios for Catalyst 6500 Series Switches in Metro Edge



- *Grid computing network*—Provides high-speed optical interface modules and world-class software required to handle high-volume traffic and build and manage large-scale networks

Figure 5
Deployment Scenarios for Catalyst 6500 Series Switches in Grid Computing Network



6.120
W

System Overview

Modular Architecture

The Cisco Catalyst 6500 Series is a modular system that can grow as customer requirements expand and technology evolves, allowing customers to upgrade and reconfigure systems by adding new modules, replacing existing modules, and adding and redeploying systems. Throughout the Cisco Catalyst 6500 Series, modules are:

- *Configurable*—Separately, simplifying the addition of new services
- *Interoperable*—In the same chassis, providing flexible design options
- *Interchangeable*—Among Cisco Catalyst 6500 Series systems, simplifying sparing and network expansion
- *Hot-swappable*—Without requiring a chassis to be powered off, providing fast upgrade and repair
- *Upgradable*—As newer modules come along, providing investment protection

Cisco Catalyst 6500 Series Hardware-Forwarding Architectures

Cisco Catalyst 6500 Series modules use one of three forwarding technologies, each having a different architecture with different characteristics and capabilities:

- *Cisco Express Forwarding (CEF)*—Scaling to 30 Mpps, this technology uses a central CEF Cisco Express Forwarding engine located on the supervisor engine's policy feature card (PFC) daughter and CEF forwarding tables located on the supervisor engine. The supervisor engine makes all forwarding decisions for all interface modules centrally. For more information see *How Cisco Express Forwarding Works.*
- *Accelerated Cisco Express Forwarding (aCEF)*—Suited for high-performance enterprise environments, this technology uses the aCEF engine and aCEF tables located on the interface module, along with the central CEF engine located on the supervisor engine's PFC daughter card and central CEF forwarding tables located on the supervisor engine. The interface module makes high-volume forwarding decisions locally, and the supervisor engine makes the rest of the forwarding decisions centrally. For more information see *How Accelerated Cisco Express Forwarding (aCEF) Works.*
- *Distributed Cisco Express Forwarding (dCEF)* —Suited for the most demanding environments, this technology uses the dCEF engine located on the interface module's distributed forwarding card (DFC) daughter card and the dCEF table, a local copy of the supervisor engine's central CEF table located on the interface module's DFC. The interface module makes all the forwarding decisions locally, and provides maximum performance and scalability. For more information see *How Distributed Cisco Express Forwarding (dCEF) Works*

Cisco Catalyst 6500 Series Switching Architectures

Cisco developed the following switching architectures for Cisco Catalyst 6500 modules to allow platforms to scale in any deployment:

- 32-Gbps bus—Allowing access to a central shared bus
- 256-Gbps switch fabric—Located on the switch fabric module (SFM)
- 720 Gbps switch fabric—Located on Cisco Catalyst 6500 Series Supervisor Engine 720

Cisco Catalyst 6500 Series Modules

Cisco Catalyst 6500 Series interfacecmodules support the following forwarding technology and switch fabric combinations:

- *Classic Interface Modules*—Use the centralized CEF engine located on the supervisor engine's PFC, connect to the 32-Gbps switching bus only, and forward packets at up to 15 Mpps
- *CEF256 Interface Modules*—Use the centralized CEF engine located on the supervisor engine's PFC, connect to both the 256-Gbps fabric located on the supervisor engine with a single 8-Gbps full-duplex fabric connection and the 32-Gbps switching bus, and forward packets at up to 30 Mpps
- *dCEF256 Interface Modules*—Use the distributed CEF engine on the DFC (located on the interface module), connect to a 256-Gbps fabric located on the supervisor engine or a Switch Fabric Module with 16-Gbps full-duplex fabric connections, and forward packets at up to 210 Mpps
- *aCEF720 Interface Modules*—Use the accelerated CEF engine on the DFC3 (located on the interface module), connect to the 720-Gbps fabric located on the supervisor engine with 40-Gbps full-duplex fabric connections, and forward packets at up to 400 Mpps, peak performance
- *dCEF720 Interface Modules*—Use the distributed CEF engine on the DFC3 (located on the interface module), connect to the 720-Gbps fabric located on the supervisor engine with dual 20-Gbps full-duplex fabric connections, and forward packets at up to 400 Mpps, sustained performance

Note: All Performance numbers refer to IPv4 forwarding.

Cisco Catalyst 6500 Series Module Types

In the Cisco Catalyst 6500 Series architecture, special-purpose modules perform separate tasks—allowing the feature set to evolve quickly and allowing customers to add new features and enhanced performance by adding new modules. The Cisco Catalyst 6500 Series features the following types of special-purpose modules:

- *Supervisor engines*—Perform the control functions and make the forwarding decisions for packets routed to other networks
- *Ethernet interface modules*—Provide IEEE-standard receive and forwarding interfaces and forward packets within the defined network
- *WAN interface modules*—Provide the receive and forwarding interface at the WAN edge
- *Services modules*—Support multigigabit security, application-aware Layer 4 through 7 content switching, network management, and voice gateway services to traditional phones, fax machines, PBXs, and the PSTN
- *Switch Fabric Modules (SFMs)*—Pass network traffic from interface module to the supervisor engine or to another interface

Cisco Catalyst 6500 Series Supervisor Engines

The supervisor engines for the Cisco Catalyst 6500 Series support different forwarding technologies and achieve different forwarding rates, depending on the configuration of the supervisor engine and the capability of a particular interface module.

Supervisor engines can be configured with optional factory-installed daughter cards—a Policy Feature Card (PFC) providing hardware-based Layer-2 forwarding, and a Multilayer Switch Feature Card (MSFC) providing Layer 3 capabilities.

A supervisor engine performs control operations centrally on processors that run either Cisco IOS Software or Cisco Catalyst Operating System Software while special-purpose application-specific integrated circuits (ASICs) perform bridging and routing (based on Cisco Express Forwarding), QoS marking and policing, and access control. The same ASICs are used on the DFCs, daughter cards that can be installed on certain interface modules to distribute forwarding in a decentralized fashion to achieve system forwarding rates of up to 400 Mpps (Table 2).

For additional information about the following Cisco Catalyst 6500 Series supervisor engines visit: http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet

Table 2 Cisco Catalyst 6500 Supervisor Engines

Feature	Supervisor Engine 1	Supervisor Engine 2	Supervisor Engine 7
Solution and market	Wiring closet	Enterprise distribution, core, and WAN edge; service provider WAN and Internet edge	Enterprise core and data center; service provider metro; wireless; national research networks; grid computing
Fabric architectures supported	Centralized forwarding only—engine located on supervisor engine's PFCx daughter card	Centralized CEF—engine located on supervisor engine's PFCx daughter card; Distributed CEF—engine located on interface module's DFC daughter card	Centralized CEF—engine located on Supervisor Engine 720's PFC3 daughter card; Distributed CEF—engine located on interface module's DFC3 daughter card; Accelerated CEF—engine located on interface module's ASICs
Fabric connections	32-Gbps shared bus connection to modules	16 Gbps per slot; Dual-fabric connection to modules at 8 Gbps full duplex per channel	40 Gbps per slot; Dual-fabric connection to modules at 20 Gbps full duplex per channel
Performance maximum (Mpps)	15 Mpps	210 Mpps	Sustained 400 Mpps—dCEF720 Peak 400 Mpps—aCEF720
DFC modules	Not supported	DFC	DFC3

Table 2 Cisco Catalyst 6500 Supervisor Engines

Feature	Supervisor Engine 1	Supervisor Engine 2	Supervisor Engine 720
Route processor	On MSFC2 daughter card (optional)	On MSFC2 daughter card (optional)	MSFC3 integrated
PFC modules	PFC daughter card (optional)	PFC2 integrated	PFC3 integrated

Ethernet Interface Modules

Cisco Catalyst 6500 Series Ethernet interface modules, designed for wiring closet, distribution and core, and data center applications, as well as service provider and Metro Ethernet environments, use one of the following types of Ethernet interfaces:

- *10/100 Mbps over copper and 10/100/1000 Mbps Ethernet over copper*—For wiring closets providing 10/100- and 10/100/1000-Mbps performance with auto-negotiation and inline power for voice; up to 48 ports/module; includes Classic and CEF256 interface modules.
- *100 Mbps over fiber*—For secure wiring closets and long-haul router and switch interconnects; up to 24 ports per module; includes Classic and CEF256 interface modules.
- *1 Gbps*—For distribution and core layers and for data centers providing 1-Gbps performance in a 48-port module; includes Classic CEF256, and dCEF256 interface modules.
- 10 Gbps—For distribution and core layers providing 10-Gbps performance in 1-port or 2-port module; includes CEF256, aCEF720, and dCEF720 interface modules.

For more information, visit:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

WAN Interface Modules

The Cisco Catalyst 6500 Series and Cisco 7600 Series support several WAN interfaces using two technologies:

- *FlexWAN module*—Accepts up to two plug-in port adapters that provide numerous WAN/MAN protocols and features
- *Optical Services Module (OSM)*—A dedicated line card that provides several interfaces, including OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, Channelized T3, Channelized OC-12/STM-4 PoS, Gigabit Ethernet, OC-12/STM-4 ATM, and OC-48/STM-16 Dynamic Packet Transport (DPT)

FlexWAN Module

The FlexWAN module fits inside Cisco Catalyst 6500 Series and Cisco 7600 Series systems and uses Cisco 7200 and 7500 Series port adapters for a wide range of WAN/MAN protocols, including Frame Relay, ATM, PoS, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC). Additionally, the FlexWAN module provides media options such as clear channel and Channelized T1/E1, T3/E3, High-Speed Service Interface (HSSI), OC-3 PoS, and ATM.

- For information about the Cisco Catalyst 6500 Series and Cisco 7600 Series FlexWAN Module, visit: http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a00800923bf.html

Optical Services Modules

OSMs are line cards that provide high-speed WAN connectivity with onboard network processors for distributed-line-rate IP service applications. For more information about OSMs, see the following data sheets:

- Cisco 7600 Series 4-, 8-, and 16-Port OC-3c/STM-1 PoS/SDH OSM:
  http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092249.html
- Cisco 7600 Series 4-Port Gigabit Ethernet OSM:
  http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008009223d.html
- Cisco 7600 Series 1-Port Channelized OC-12/STM-4 to DS3/E3 OSM:
  http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092250.html
- Cisco 7600 Series 1-Port OC-48c/STM-16 PoS/SDH/OSM:
  http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080092241.html
- Cisco 7600 Series 2- and 4-Port OC-12c/STM-4 PoS/SDH OSM:
  http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008009223e.html
- Cisco 7600 Series 2-Port ATM OSM:
  http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a008008876f.html
- Cisco 7600 Series 2-Port OC-48c/1-Port OC-48c DPT OSM:
  http://www.cisco.com/en/US/products/hw/routers/ps368/products_data_sheet09186a0080088774.html
  Layer 4 Through 7 Services Modules

The Cisco Catalyst 6500 Series offers an extensive set of services modules for Layer 4 through 7 applications, including content services, network monitoring, security, and telephony.

Content Services Modules

- *Content Services Gateway (CSG)*—Enables differentiated billing, user balance enforcement, and activity tracking for customer billing systems. For more information, visit: http://mobiletraining.cisco.com/csg/CSGe_ds_0211.pdf
- *Content Switching Module (CSM)*—Integrates advanced content switching into the Cisco Catalyst 6500 Series to provide high-performance, high-availability load balancing of caches, firewalls, Web servers, and other network devices. For more information, visit:
  http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800887f3.html

Network Monitoring

- *Network Analysis Module (NAM 1 and 2)*—Provides application-level visibility into the network infrastructure for real-time traffic analysis, performance monitoring, and troubleshooting; performs traffic monitoring with embedded Web-based traffic analyzer. For more information, visit:
  http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800a2c89.html

Security Services Modules

- *Firewall Services Module (FWSM)*—The FWSM allows any port in the chassis to operate as a firewall port and integrates stateful firewall security inside the network infrastructure. For more information, visit:
  http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09 186a00800c4fe7.html
  Intrusion Detection System Module (IDSM and IDSM-2)—Takes traffic from the switch backplane at wire speed, integrating IDS functions directly into the switch. For more information, visit:
  http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a0080092341.html

- *IPSec VPN Module (IVSM)*—Provides infrastructure-integrated IPSec VPN services capable of 1.9-Gbps Triple Data Encryption Standard (3DES) performance, 8000 active tunnels, and up to 60 tunnels per second. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09 186a00800c4fe2.html
- *SSL Services Module (SSM)*—Offloads processor-intensive tasks related to securing traffic with SSL accelerating the performance and increasing the security of Web-enabled applications. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet09186a00800c4fe9.html

Telephony Services Modules

- *Communications Media Module (CMM)*—Provides flexible, high-density T1 and E1 gateways, allowing organizations to connect their existing time-division multiplexing (TDM) networks to their IP communications networks, and providing connectivity to the PSTN. For more information, visit: http://www.cisco.com/en/US/products/hw/modules/ps3115/products_data_sheet09 186a00800e9c1f.html

Switch Fabric Modules

Designed to support distributed forwarding for interface modules that have distributed forwarding capability, the Cisco Catalyst 6500 Series SFM or SFM2, in combination with the Cisco Catalyst 6500 Series Supervisor Engine 2-MSFC2 and DFCs on interface modules, increases available system bandwidth from 32 to 256 Gbps. The SFM/ SFM2 supports the Cisco Catalyst 6500 CEF256 and dCEF256 interface modules.

Designed to support new interface modules with 720 Gbps forwarding capabilities, the Supervisor Engine 720's onboard switch fabric increases available bandwidth to 720 Gbps and enables packet forwarding rates up to 400 Mpps. By using auto-sensing and auto-negotiation, the Supervisor 720 switch fabric is fully interoperable with the 8- and 16-Gbps switch fabric interconnections used by the CEF256 and dCEF256 interface modules. When a CEF256 or dCEF256 interface module is detected, the switch fabric will automatically connect those modules by offering 8-16 Gbps of bandwidth to each module, as applicable.

How Cisco Express Forwarding Works

Cisco Express Forwarding (CEF) is a Layer 3 technology that provides increased forwarding scalability and performance to handle many short-duration traffic flows common in today's enterprise and service provider networks. To meet the needs of environments handling large amounts of short-flow, Web-based, or highly interactive types of traffic, CEF forwards all packets in hardware, and maintains its forwarding rate completely independent of the number of flows going though the switch.

On the Cisco Catalyst 6500 Series, the CEF Layer 3 forwarding engine is located centrally on the supervisor engine's PFC2 or PFC3—the same device that performs hardware-based Layer 2 and 3 forwarding, ACL checking, QoS policing and marking, and NetFlow statistics gathering.

Using the routing table that Cisco IOS Software builds to define configured interfaces and routing protocols, the CEF architecture creates CEF tables and downloads them into the hardware-forwarding engine before any user traffic is sent through the switch. The CEF architecture places only the routing prefixes in its CEF tables—the only information it requires to make the Layer 3 forwarding decisions—relying on the routing protocols to do route selection. By performing a simple CEF table lookup, the switch forwards packets at wire-rate, independent of the number of flows transiting the switch.

CEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 2 or Catalyst Supervisor Engine 720.

How Accelerated Cisco Express Forwarding (aCEF) Works

Accelerated Cisco Express Forwarding (aCEF) technology uses two forwarding engines working together in a master-slave relationship to accelerate high-rate traffic flows through the switch—a central CEF engine located on the Supervisor Engine 720's PFC3 and a scaled-down distributed aCEF engine located on the interface module.

The central PFC3 makes the initial forwarding decision, with the aCEF engine storing the result and making subsequent packet-forwarding decisions locally. aCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 is loaded with the necessary CEF information before any user traffic arrives at the switch.
- As traffic arrives on an aCEF720 interface module, the aCEF engine inspects the packet, and finding that no specific packet forwarding information exists, consults the central PFC3.
- The PFC3 makes a hardware-based forwarding decision for this packet (including Layer 2, Layer 3, ACLs, and QoS).
- The aCEF engine stores the forwarding decision results and makes forwarding decisions locally for subsequent packets based on packet-flow history.
- The aCEF engine handles hardware-based Layer 2 and Layer 3 forwarding, ACLs, QoS marking, and NetFlow.
- The central PFC3 processes any forwarding decisions that the interface module's aCEF engine cannot handle.

aCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 and aCEF720 (WS-X67xx) class modules.

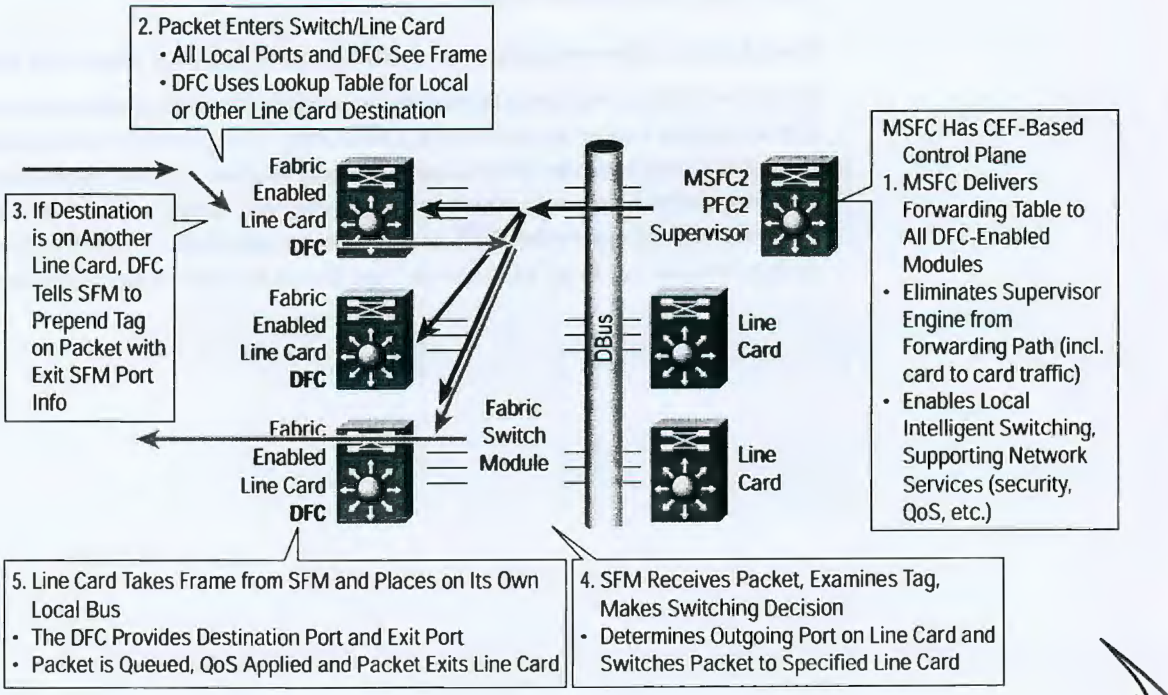
How Distributed Cisco Express Forwarding (dCEF) Works

With Distributed Cisco Express Forwarding (dCEF), forwarding engines located on the interface modules make forwarding decisions locally and in parallel, allowing the Cisco Catalyst 6500 Series to achieve the highest forwarding rates in the industry. With dCEF, forwarding occurs on the interface modules in parallel and system performance scales up to 400 Mpps—the aggregate of all forwarding engines working together.

Using the same ASIC engine design as the central PFCx, DFCs located on the interface modules forward packets between two ports, directly or across the switch fabric, without involving the supervisor engine. With the DFC, each interface module has a dedicated forwarding engine complete with the full forwarding tables. dCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 located on the supervisor engine and the DFC engines located on the interface modules are loaded with the same CEF information derived from the forwarding table before any user traffic arrives at the switch.
- As a packet arrives at an interface module, its DFC engine inspects the packet and uses the information in the CEF table (including Layer 2, Layer 3, ACLs, and QoS) to make a completely hardware-based forwarding decision for that packet.
- The dCEF engine handles all hardware-based forwarding for traffic on that module, including Layer 2 and Layer 3 forwarding, ACLs, QoS policing and marking, and NetFlow.
- Because the DFCs make all the switching decisions locally, the supervisor engine is freed from all forwarding responsibilities and can perform other software-based functions, including routing, management, and network services.

Figure 6
Distributed Cisco Express Forwarding Packet Flow


Fabric Enabled Line Card DFC
Fabric Enabled Line Card DFC
Fabric Enabled Line Card DFC
Fabric Switch Module
DBus
MSFC2 PFC2 Supervisor
Line Card
Line Card

2. Packet Enters Switch/Line Card
- All Local Ports and DFC See Frame
- DFC Uses Lookup Table for Local or Other Line Card Destination

3. If Destination is on Another Line Card, DFC Tells SFM to Prepend Tag on Packet with Exit SFM Port Info

MSFC Has CEF-Based Control Plane
1. MSFC Delivers Forwarding Table to All DFC-Enabled Modules
- Eliminates Supervisor Engine from Forwarding Path (incl. card to card traffic)
- Enables Local Intelligent Switching, Supporting Network Services (security, QoS, etc.)

5. Line Card Takes Frame from SFM and Places on Its Own Local Bus
- The DFC Provides Destination Port and Exit Port
- Packet is Queued, QoS Applied and Packet Exits Line Card

4. SFM Receives Packet, Examines Tag, Makes Switching Decision
- Determines Outgoing Port on Line Card and Switches Packet to Specified Line Card

dCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 for the dCEF720 interface module; requires either a Catalyst Supervisor Engine 720 or a Catalyst Supervisor Engine 2-MSFC2 and a SFM for the dCEF256 interface module.

Cisco IOS Software and Catalyst Operating System Software

Cisco Catalyst 6500 Series switches offer two operating modes of software, the Cisco Catalyst Operating System Software with optional Cisco IOS Software on the MSFC, and Cisco IOS Software for the supervisor engines. Each operating mode can be deployed at different hierarchies of the network, depending on the network's requirements. These software solutions for the Cisco Catalyst 6500 Series switches provide full Layer 2 through 4 switching and routing functions at high performances.

Today, either of these operating modes can be deployed in an entire network environment, or the operating modes can vary within an environment to meet different requirements. One operating mode is not a replacement for another, but is recommended for varying feature requirements.

- Cisco IOS Software for the Cisco Catalyst 6500 Series
- Cisco Catalyst Operating System Software with optional Cisco IOS Software on the MSFC

Cisco IOS Software for the Cisco Catalyst 6500 Series

Cisco IOS Software for the Cisco Catalyst 6500 Series supervisor engines requires the MSFC on the supervisor engine. It provides integrated multilayer functions in a single image and is optimized for core, distribution, Internet access, and data center deployments. Cisco IOS Software combined with the performance of the Cisco Catalyst 6500 Series offers the necessary features for a high-performance Layer 3-enabled deployment, including support for a distributed architecture with the ability to scale the switch to 400 Mpps throughput. Additionally, Cisco IOS Software provides operational ease of use by offering a single image and configuration file to be deployed across the Cisco Catalyst 6500 Series switches.

Cisco Catalyst Operating System Software with Optional Cisco IOS Software on the MSFC

Cisco Catalyst Operating System Software is the premier software for the wiring closet on Cisco Catalyst 6500 Series switches offering high-performance Layer 2 forwarding. It is optimized to deliver the high availability, enhanced security, and integrated inline power support necessary for mission-critical wiring closet deployments. Cisco Catalyst Operating System Software can also be extended to the distribution and core layers of the network when coupled with Cisco IOS Software on the MSFC, providing robust and advanced Layer 3 and Layer 4 functions. This operating mode is often referred to as "hybrid mode." See Table 3 for software and hardware deployment options.

Table 3 Software and Hardware Deployment Options

Network Performance	Wiring Closet	Distribution/ Data Center	Core	WAN Edge
Highest-performance Cisco IOS Software end-to-end	Cisco IOS Software; Supervisor Engine 2-MSFC2; CEF256 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 and aCEF720 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF720 and aCEF720 interface modules
Higher-performance mixed operating system	Cisco Catalyst Operating System Software; Supervisor Engine 2-PFC2; CEF256 and Classic interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF256 and CEF256 interface modules	Cisco IOS Software; Supervisor Engine 720; dCEF720 and aCEF720 interface modules	Cisco IOS Software; Supervisor Engine 2-MSFC2; dCEF256 and, CEF256 interface modules
High-performance Cisco Catalyst Operating System Software end-to-end	Cisco Catalyst Operating System Software; Supervisor Engine 1-2GE; CEF256 and Classic interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; CEF256 and Classic interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; dCEF720 Series and aCEF720 interface modules	Hybrid mode; Supervisor Engine 2-MSFC2; CEF256 and Classic interface modules

Cisco IOS Software and Cisco Catalyst Operating System Software Shared Features

All Cisco Catalyst 6500 Series supervisor engines, including the new Supervisor Engine 720, take advantage of the industry-leading software and management capabilities of the Cisco Catalyst 6500 Series. Customers can apply their knowledge of Cisco Catalyst Operating System Software, Cisco IOS Software, CiscoWorks, and other graphical and Web-based network management tools without the need to learn a new command-line interface (CLI) or management system.

Cisco Catalyst 6500 Series Chassis

Cisco Catalyst 6500 Series chassis can be deployed in the wiring closet, the distribution and core layers, the data center, and the WAN edge, providing the power and features required for end-to-end deployment for the enterprise campus, the ISP network, metro, and research computing networks.

Chassis Applications

The Cisco Catalyst 6500 Series provides a selection of chassis, including 3-, 6-, 9-, and 13-slot models with slots arranged horizontally and a 9-slot model with slots arranged vertically, with front-to-back airflow. Typical applications for Cisco Catalyst 6500 Series chassis include:

- *3-slot chassis*—Low-density, wiring-closet chassis sharing interface modules and supervisor engines with larger chassis for common sparing; low-density, high-performance specialized services modules chassis for network security and management; low-density, high-end chassis providing connectivity to the WAN edge
- *6- and 9-slot chassis*—Traditional chassis for the wiring closet, distribution and core, data center, and WAN
- *13-slot chassis*—Highest-capacity chassis for Ethernet connectivity, with slots to spare for services modules providing network security and management

Chassis Configuration

All Cisco Catalyst 6500 Series chassis are NEBS Level-3 compliant and use common power supplies. The 6- and 9-slot chassis require a 1000W or 1300W power supply and the 13-slot chassis requires a 2500W or 4000W power supply. The 3-slot chassis requires a 950W power supply. When ordering a Cisco Catalyst 6500 Series switch, use the online Cisco Dynamic Configuration Tool to assist you in selecting the chassis, power supplies, power cables, and fan trays that will meet your requirements. The tool is available at: http://www.cisco.com/appcontent/apollo/configureHomeGuest.html

Power

All Cisco Catalyst 6500 chassis hold up to two load-sharing, fault-tolerant, hot-swappable AC or DC power supplies. Only one supply is required to operate a fully loaded chassis. If a second supply is installed, it operates in a load-sharing capacity. The power supplies are hot-swappable—a failed power supply can be removed without powering off the system.

Cisco Catalyst 6500 Series switch power supplies are available in five power ratings:

- 950W AC input (Cisco Catalyst 6503 chassis)
- 1000W AC input
- 1300W AC and DC input
- 2500W AC and DC input
- 4000W AC input

Table 4 outlines the power requirements and heat dissipation for the three different models of power supplies available for the Cisco Catalyst 6500 Series switch.

Table 4 Power Supply VAC and VDC requirements

Power Supply	AC Input Voltage/Current	DC Input Voltage/Current
950W	100 to 240 VAC (10% for full range); 15 A	-48 VDC to –60 VDC continuous; 38 A @ –48 VDC, 30 A @ –60 VDC
1000W	100 to 240 VAC (10% for full range); 12 A @ 100 VAC, 6 A @ 240 VAC	Not supported
1300W	100 to 240 VAC (10% for full range); 17.25 A @ 100 VAC, 8 A @ 200 VAC	–48 VDC to –60 VDC continuous; 38 A @ –48 VDC, 30 A @ –60 VDC

2500W	100 to 120 VAC, 200 to 240 VAC (10% for full range);
	16 A maximum at 200 VAC at 2500 W output;
	16 A maximum at 100 VAC at 1300 W output
		–48 VDC to –60 VDC continuous;
		80 A @ –40.5 VDC, 70 A @ –48 VDC,
		55 A @ –60 VDC

4000W	100 to 240 VAC (10% for full range); 23 A	Not supported

Fan Trays

Chassis that have a Supervisor Engine 720 installed require a high-speed fan tray. See Table 5 for part number information.

Table 5 Catalyst 6500 Chassis Fan Tray Part Numbers

Catalyst 6500 Chassis	Normal Speed Fan— Fan Tray Part Number	High Speed Fan— Fan Tray Part Number
6503	FAN-MOD-3	FAN-MOD-3-HS(=)
6506	WS-C6K-6SLOT-FAN	WS-C6K-6SLOT-FAN2
6509	WS-C6K-6SLOT-FAN	WS-C6K-9SLOT-FAN2
6509-NEB	WS-C6509-NEB-FAN	WS-C6509-NEB-FAN2
6509-NEB-A	N/A	FAN-MOD-09(=)
6513	WS-C6K-13SLOT-FAN	WS-C6K-13SLOT-FAN2

Dimensions

Table 6 provides Catalyst 6500 Series chassis dimensions.

Table 6 Catalyst 6500 Series Chassis Dimensions

Dimension	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
H x W x D (in.)	7 x 17.37 x 21.75 in.	20.1 x 17.2 x 18.1 in.	25.2 x 17.2 x 18.1 in.	33.3 x 17.2 x 18.1 in.	33.3 x 17.3 x 18.1 in.
H x W x D (cm)	17.8 x 44.1 x 55.2 cm	51.1 x 43.7 x 46.0 cm	64.0 x 43.7 x 46.0 cm	84.6 x 43.7 x 46.0 cm	84.6 x 43.7 x 46.0 cm

Table 6 Catalyst 6500 Series Chassis Dimensions

Dimension	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
Rack units (RU); 1.75 in., 4.4 cm	4 RU	12 RU	15 RU	20 RU	20 RU

Weight

Table 7 provides the weight information for empty and fully configured Catalyst 6500 Series chassis.

Table 7 Catalyst 6500 Series Chassis Weights

Weight	Cisco Catalyst 6503	Cisco Catalyst 6506	Cisco Catalyst 6509	Cisco Catalyst 6509-NEB	Cisco Catalyst 6513
Chassis only (lb)	27	45	55	55	98
Fully configured (lb)	83	115	135	135	240
Chassis only (kg)	12	20	25	25	45
Fully configured (kg)	38	52	61	61	109

Ordering Information

Table 8 provides part number information for Catalyst 6500 Series chassis

Table 8 Catalyst 6500 Series Chassis Part Numbers

Part Number	Chassis
WS-C6503	Cisco Catalyst 6503 chassis (three slots)
WS-C6506	Cisco Catalyst 6506 chassis (six slots)
WS-C6509	Cisco Catalyst 6509 chassis (nine slots)
WS-C6509-NEB	Cisco Catalyst 6509-NEB chassis (nine vertically oriented slots)
WS-C6509-NEB-A	Cisco Catalyst 6509-NEB chassis (nine vertically oriented slots)–enhanced
WS-C6513	Cisco Catalyst 6513 chassis (13 slots)

Environmental Conditions

Table 9 provides environmental information for Catalyst 6500 Series Chassis.

Table 9 Catalyst 6500 Series Chassis Environmental Conditions

Parameter	Performance Range
Operating temperature	32 to 104 F (0 to 40 C)
Storage temperature	–4 to 149 F (–20 to 65 C)
Relative humidity	10 to 90%, noncondensing
Operating altitude	3000 meters
Mean time between failure (MTBF)	7 years for system configuration

6.105
2

Regulatory Compliance

Safety

- UL 1950
- EN 60950
- CSA-C22.2 no. 950
- IEC 60950
- AS/NZA 3260
- 21 CFR 1040
- EN 60825-1
- IEC 60825-1
- TS 001

EMC

- FCC (CFR 47, Part 15) Class A
- VCCI
- CE Marking
- EN 55022
- EN 55024
- CISPR 22
- AS/NZS 3548
- NEBS Level 3 (GR-1089-CORE, GR-63-CORE)
- ETSI ETS-300386-2

Specifications

Table 10 provides an overview of Catalyst 6500 Series switches specifications, additional information can be found in software release notes.

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
IEEE Compliance		
802.1	802.1d 802.1p, q 802.1s 802.1w 802.1x	Bridging VLAN tagging Per-VLAN Group Spanning Tree Protocol Rapid Spanning Tree Protocol
802.1	802.3	10BASE-T, 10BASE-FL
	802.3ad 802.3ab 802.3ae 802.3u	Link aggregation 1000BASE-T 10 Gigabit Ethernet 100BASE-TX, 100BASE-FX
	802.3x	Flow control
	802.3z	1000BASE-SX, 1000BASE-LX
RFC Compliance		
ATM	1483, 2584	Protocol encapsulation over ATM AAL-5
		ATM permanent virtual circuit (PVC) to 802.1q tagging
BGP4	1269	Definitions of Managed Objects for the Border Gateway Protocol (Version 3)
	1745	Border Gateway Protocol/Open Shortest Path First (BGP/OSPF) interactions
	1771	BGPv4
	1965	BGP4 autonomous system confederations
	1966	BGP4 route reflection
	1997	Communities attribute
	2385	Transmission Control Protocol (TCP) MD5 authentication for BGP
	2439	Route flap dampening
	2796	Route reflection
	2842	Capabilities advertisement
General routing protocols	768	User Datagram Protocol (UDP)
	783	Trivial File Transfer Protocol (TFTP)
	791	IP

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
	792	Internet Control Message Protocol (ICMP)
	793	TCP
	826	Address Resolution Protocol (ARP)
	854	Telnet
	894	IP over Ethernet
	903	Reverse Address Resolution Protocol (RARP)
	906	TFTP Bootstrap
	951, 1542	BootP, BootP extensions
	1027	Proxy ARP
	1122	Host requirements
	1256	ICMP Router Discovery Protocol (IRDP) IPv4 router discovery
	1519	Classless interdomain routing (CIDR)
	1541	Dynamic Host Control Protocol (DHCP)
	1591	Domain Name System (DNS) client
	1619	PPP over SONET
	1662	PPP HDLC-like framing
	1812	IPv4
	2131	BootP/DHCP
	2338	VRRP
		Internetwork Packet Exchange Routing Information Protocol/ Service Advertising Protocol (IPX RIP/SAP)
		Software-controlled redundant ports
IP multicast	1112	Internet Group Management Protocol (IGMP)
	1122 2236	Host extensions, Distance Vector Multicast Routing Protocol (DVMRP) IGMP v1, v2, v3 IGMP v1, v2, v3 Snooping
	2283	Multicast Border Gateway Protocol (MBGP)
	2362	Protocol-Independent Multicast (PIM)-SM
		DVMRP v3-07 Multicast Source Discovery Protocol (MSDP)
		PIM-Dense Mode (PIM-DM) v1

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
		PIM-DM v2 Bidirectional PIM (Supervisor Engine 720 only)
Intermediate system to Intermediate system (IS-IS)	1195	TCP
	1377	PPP
	2763	Dynamic host name exchange
	2966	Domain-wide prefixes
LSP tunnels	2211	Controlled load network element service
	2702	Traffic engineering over MPLS
MPLS	2547	MPLS VPN
	2961	Resource Reservation Protocol (RSVP) refresh
	3031	MPLS architecture
	3032	MPLS label stack encoding
	3036	Label Distribution Protocol (LDP)
OSPF	1583	OSPF v2
	1587	OSPF NSSA
	1745	OSPF interactions
	1765	OSPF database overflow
	1850	OSPF v2 Management Information Base (MIB), traps
	1997	Communities and attributes
	2154	OSPF digital signatures, MD5
	2178	OSPF v2 (superceded by RFC 2328)
	2328	OSPF v2
	2370	OSPF opaque link-state advertisement (LSA) option
	2385	TCP M5
	2439	Route flap damping
	2842	Capabilities advertisement
	2918	Route refresh capability
RIP	1058	RIP v1
	1723	RIP v2
	2453	RIP v2

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
Miscellaneous protocols	1866	HTML
	2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
	2068	HTTP
Denial of service (DoS) protection	2267	Network Ingress Filtering
		ACLs: wire-speed
		ICMP and IP-option control
		IP broadcast forwarding control
		Rate limiting using ACLs
		Unicast Reverse Path Forwarding (RPF)
		Server load balancing with Layer 3 and Layer 4 protection
		SYN attack protection
		Session control
Network management	782	VLAN Trunking Protocol (VTP)
	783	TFTP
	854	Telnet
	951	BOOTP
	1155	Structure of Management Information (SMIv1)
	1156	TCP/IP MIB
	1157	Simple Network Management Protocol (SNMP)v1
	1212	MIB definitions
	1213	SNMP MIB II
	1215	SNMP traps
	1256	ICMP router discovery
	1285	Station management (SMT) 7.3
	1354	IP forwarding table MIB
	1493	Bridge MIB
	1516	Ethernet repeater MIB
	1573	Interface table MIB
	1643	Ethernet MIB
	1650	Ether-like MIB

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
	1657	BGPv4 MIB
	1724	RIPv2 MIB
	1757	RMON MIB
	1850	OSPFv2 MIB
	1901, 1907	SNMPv2c
	1908	SNMPv1/v2 coexistence
	2021	RMON2 probes
	2037	ENTITY-MIB
	2096	IP forwarding
	2233	Interface MIB
	2613	RMON analysis for switched networks (SMON) MIB
	2668	802.3 media attachment unit (MAU) MIB
	2787	VRRP MIB
	2925	Ping/Traceroute/NS Lookup MIB
		Sampled Netflow
		999 local messages
		BSD Syslog with multiple servers
		Configuration logging
		CISCO-CDP-MIB
		CISCO-COPS-CLIENT-MIB
		Cisco Discovery Protocol
		CISCO-ENTITY-FRU-CONTROL-MIB
		CISCO-PAGP-MIB
		CISCO-STACK-MIB
		CISCO-STP-Extensions-MIB
		Cisco Traffic Director Software
		CISCO-UDLDP-MIB
		CiscoView
		CISCO-VLAN-Bridge-MIB
		Cisco VLAN Director Software
		CISCO-VLAN-Membership-MIB

6099
L

Table 10 Catalyst 6500 Series Specifications

Specification	Number	Description
		CISCO-VTP-MIB
		Cisco Workgroup MIB
		SPAN and Remote SPAN (RSPAN)
		Hot Standby Routing Protocol (HSRP)
		HC-RMON
		HTML/HTTP management
		NetFlow v1 export
		RMON HP Open View
		SMON-MIB
		Standard Cisco IOS Software security capabilities: passwords and TACACS+
		Telnet client
		Telnet management
		Text-based CLI
		Web-based GUI Management Tools (CiscoWorks)
Security	1492	Terminal Access Controller Access Control System Plus (TACACS+)
	2138	Remote Authentication Dial-In User Service (RADIUS) authentication
		ACLs for Layers 2, 3, 4, and 7
		Access profiles on all routing protocols
		Access profiles on all management methods
		Media Access Control (MAC) address security/lockdown
		Network Address Translation (NAT)
		Network login (including DHCP/RADIUS integration)
		RADIUS accounting
		RADIUS per-command authentication
		Secure Copy Protocol (secure file transfer)

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit:
http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Additional Cisco Catalyst 6500 Series Information

For additional information about the following data sheets that describe Cisco Catalyst 6500 Series, supervisor engines, interface modules, SFM, and services modules, visit:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series 10 Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series FlexWAN Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Switch Fabric Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Content Services Module Data Sheet
- Cisco Catalyst 6500 Series Firewall Services Module Data Sheet
- Cisco Catalyst 6500 Series Network Application Module (NAM) Data Sheet
- Cisco Catalyst 6500 Series Intrusion Detection (IDS) Module Data Sheet
- Cisco Catalyst 6500 Series IPSec VPN Services Module Data Sheet
- Cisco Catalyst 6500 Series SSL Services Module Data Sheet

6097

Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice EP

CISCO SYSTEMS

Data Sheet

Cisco Catalyst 6500 Series
Gigabit Ethernet Modules

The Cisco Catalyst® 6500 Series Switch—the premier modular multilayer switch—delivers secure converged services from the wiring closet to the core, to the data center, to the WAN edge.

Designed to complement the many roles that the Cisco Catalyst 6500 Series plays in a network, Cisco Catalyst 6500 Series Gigabit Ethernet modules offer the broadest selection of media, densities, performance, interoperability, and chassis deployments for enterprises and service providers. *These modules are ideal for* gigabit to the desktop, gigabit uplinks, aggregation of high-density 10/100 interfaces, Metro Ethernet links; and backbone and high-speed server farm or data center connections. The Cisco Catalyst 6500 Series Gigabit Ethernet modules offer the following features:

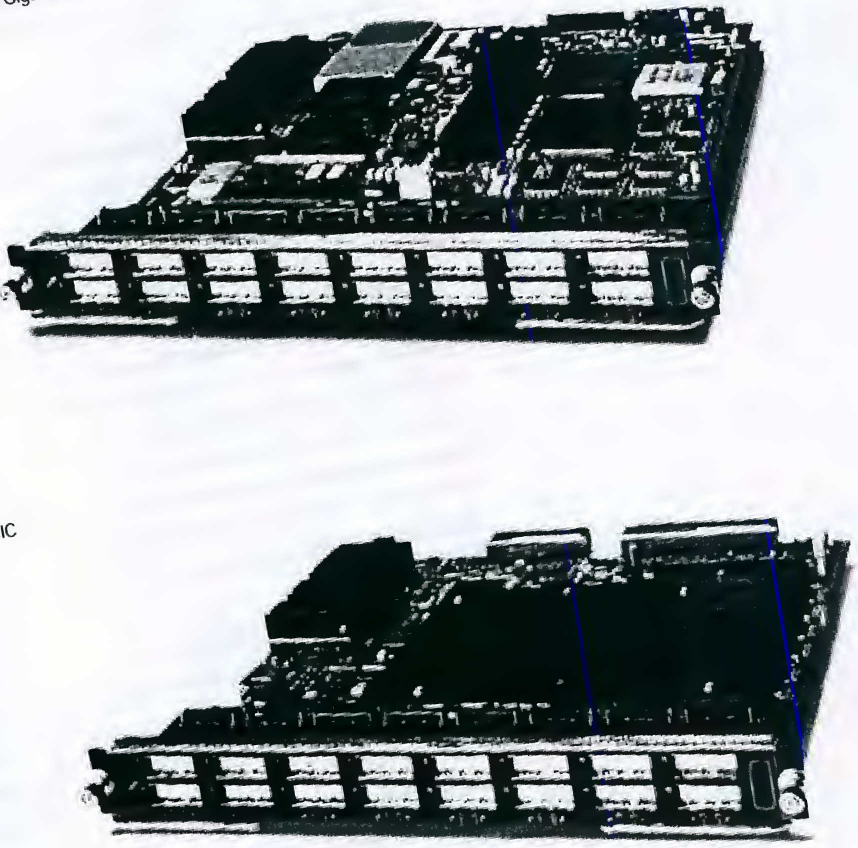
- Flexible configurations for any deployment—Provide flexible port densities, media choices, and performance speeds for any deployment requirement
- Choice of media and connector type—Available in multimode fiber or single-mode fiber using MT-RJ and modular GBIC and SFP optics supporting station-to-station distances up to 100 km

Note: For information about 10/100/1000 copper interface modules with auto-negotiation, see the Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Data Sheet

- High port densities—From 8 up to 16 ports per module, up to 256 ports per system
- Scalable and predictable performance—Provide a selection of switch fabric connections and throughput: 32 Gbps bandwidth/15 Mpps (Classic interface modules), 256 Gbps bandwidth/30 Mpps (CEF256 interface modules), and 256 Gbps bandwidth/210 Mpps (dCEF256 interface modules)
- Operational consistency—Supported in all Catalyst 6500 3-, 6-, 9-, and 13-slot chassis running Cisco IOS® Software and Cisco Catalyst Operating System Software; interoperable with all other interfaces and services modules; and forward-compatible with all Catalyst 6500 supervisor engines
- Maximum network uptime and resiliency—Support Cisco enhanced Per-Virtual LAN (VLAN) Spanning Tree Plus (PVST+) protocol, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree (MST) protocol, Per-VLAN Rapid Spanning Tree (PVRST) protocol, Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Cisco EtherChannel®, and IEEE 802.3ad link aggregation for fault-tolerant connectivity

- Superior traffic management—Available with large per-interface buffers and multiple-priority queues for traffic prioritization and policing, allowing for tight service-level agreement (SLA) enforcement
- Extensive management tools—Support CiscoWorks network management platform, Simple Network Management Protocol (SNMP) versions 1, 2, and 3 and four RMON groups (statistics, history, alarms, and events)

Figure 1
Cisco Catalyst 6500 Series Gigabit Ethernet Interface Modules



WS-X6816-GBIC

WS-X6516A-GBIC

Gigabit Ethernet Applications

Gigabit Ethernet interface modules are used in distribution and core layers, and in data-center applications (Table 1).

Table 1 Cisco Catalyst 6500 Series Gigabit Interface Module Applications

Primary Applications	Product Number	Interface Module Class	Ports/ Connector/ Interface	Queues per Port (Tx = Transmit, Rx = Receive)[1]	Buffer Size
Data center and server farm	WS-X6816-GBIC	dCEF256	16, GBIC	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Data center and server farm	WS-X6516A-GBIC	CEF256	16, GBIC	Tx–1p2q2t Rx–1p1q4t	1 MB per port
Base server farm	WS-X6408A-GBIC	Classic	8, GBIC	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Base server farm	WS-X6316-GE-TX	Classic	16, RJ-45, 1000	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Base server farm	WS-X6516-GBIC[1]	CEF256	16, GBIC	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Base server farm	WS-X6416-GBIC	Classic	16, GBIC	Tx–1p2q2t Rx–1p1q4t	512 KB per port
Base server farm	WS-X6416-GE-MT	Classic	16, MT-RJ, MM	Tx–1p2q2t Rx–1p1q4t	512 KB per port

[1] **Queues Legend:** 1p2q2t = 1 priority queue, 2 round robin queues, 2 thresholds

Gigabit Ethernet Interface Modules

The Cisco Catalyst 6500 Classic, CEF256, and dCEF26 interface modules provide Gigabit Ethernet with a choice of speeds and forwarding rates.

Classic Interface Modules

Suited for wiring closet applications, Classic interface modules use the supervisor engine for centralized Layer 2 and Layer 3 forwarding, and forward packets up to 15 Mpps over a 32-Gbps shared bus.

Capable of operating in the same chassis with the Cisco Catalyst 6500 Series Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, Catalyst Classic interface modules do not support distributed forwarding and cannot be upgraded with a Distributed Forwarding Card (DFC).

Table 2 provides more information about Catalyst Classic interface modules.

CEF256 Interface Modules

Suited for distribution and core layers and for data-center and Web-hosting applications, CEF256 interface modules use the centralized CEF engine located on the supervisor engine's policy feature card (PFC) and forward packets up to 30 Mpps over a dedicated 8-Gbps full-duplex switch fabric connection.

Capable of operating in the same chassis with the Cisco Catalyst 6500 Series Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, CEF256 interface modules support distributed forwarding when upgraded with a DFC (Table 2).

Table 2 CEF256 Interface Module Distributed Forwarding Upgrade Requirements

Supervisor Engine	Switch Fabric	Distributed Forwarding Card
Supervisor Engine 2 MSFC2/PFC2	Separate switch fabric module (SFM)	Requires WS-F6K-DFC upgrade
Supervisor Engine 720	Supervisor Engine 720 integrates a 720 Gbps switch fabric *Note:* A Supervisor Engine 720 and an SFM cannot occupy the same chassis	Requires WS-F6K-DFC3 upgrade; will not interoperate with WS-F6K-DFC

dCEF256 Interface Modules

Suited for distribution and core layers, for data-center and Web-hosting applications, and for several high-performance service provider applications, the dCEF256 interface modules use the dCEF engine and tables located on the interface module to perform all forwarding.

dCEF256 interface modules require a Cisco Catalyst 6500 Series Supervisor Engine 720 or a Supervisor Engine 2 with a Multilayer Switch Feature Card 2 (MFSC2) and SFM. Supervisor Engine 720 requires a WS-F6K-DFC3 upgrade; and Supervisor Engine 2-MFSC2 operates with the WS-F6K-DFC supplied with the dCEF256 interface module.

Table 3 Interface Module Class Comparison: Classic, CEF256, and dCEF256

Feature	Classic	CEF256	dCEF256
Performance maximum (Mpps)	15	30	210
Forwarding engine/ location	Centralized CEF Engine; located on supervisor engine's PFCx	Centralized CEF Engine; located on supervisor engine's PFCx	Distributed CEF Engine; located on interface module's DFCx

Supervisor engine supported	Supervisor Engine 1A;
	Supervisor Engine 2;
	Supervisor Engine 720
		Supervisor Engine 1A (15 Mpps maximum);
		Supervisor Engine 2;
		Supervisor Engine 720
			Supervisor Engine 2;
			Supervisor Engine 720

DFC modules integrated/ upgrade requirements	Not supported	None integrated; upgrade with WS-F6K-DFC3 for Supervisor Engine 720 *or* upgrade with WS-F6K-DFC for Supervisor Engine 2-MSFC2	DFC integrated; DFC3 field upgrade (requires Supervisor Engine 720)
Fabric connections	32 Gbps shared bus connection (on Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720)	Single 8-Gbps channel connection to switch fabric (on Supervisor Engine 720 or Supervisor Engine 2-MSFC2 with SFM) *and* 32-Gbps shared bus connection	Dual 8-Gbps full-duplex serial channel connections to switch fabric (on Supervisor Engine 720 or Supervisor Engine 2-MSFC2 with SFM)
Slot requirements	Can occupy any slot in any chassis	Can occupy any slot in any chassis	Can occupy any slot in any Cisco Catalyst 6503, 6506, 6509, 6509-NEB, or 6509-NEB-A chassis, or any Cisco 7603, 7606, 7609, or OSR-7609 chassis; can only occupy slots 9 through 13 in a 6513, or 7613 chassis
Receive queue structure	1p1q4t	1p1q4t	1p1q4t
Transmit queue structure	1p2q2t	1p2q2t	1p2q2t
Scheduler	Weighted Round Robin (WRR)	WRR	WRR
Buffer size	512 KB	512 KB or 1 MB (WS-X6516a)	512 KB

Legend: 1p2q2t = one strict priority queue, two round-robin queues, and two different thresholds

Cisco Catalyst Classic Gigabit Ethernet Copper Interface Modules

Designed for distribution and core layers and for data-center and Web-hosting applications, Cisco Catalyst Classic copper interface modules provide line-rate Gigabit Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Fabric connection—Provide a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—None; can occupy any slot in any Cisco Catalyst 6500 Series chassis

Table 4 Classic Gigabit Ethernet Copper Interface Modules

Product	Ports/Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type
WS-X6316-GE-TX	16 ports; 1000BASE-T; RJ-45	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	100 meters; Category 5 cable

Cisco Catalyst Classic Gigabit Ethernet Optical Interface Modules

Designed for distribution and core layers and for data-center and Web-hosting applications, Cisco Catalyst Classic optical interface modules provide line-rate Gigabit Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Optics—Supports hot-pluggable gigabit interface converters (GBICs)

Fabric connection—Provide a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

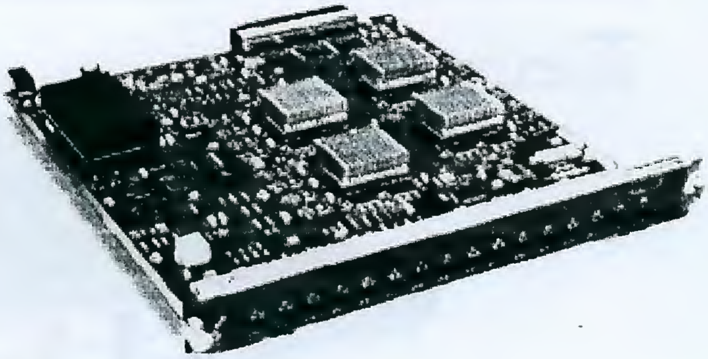
Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Table 5 Classic Gigabit Ethernet Optical Interface Modules

Product	Transceiver Type	Ports/Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type
WS-X6408A-GBIC	GBIC	8 ports; 1000BASE-SX, -LX/LH, -ZX; SC	96 ports (Cisco Catalyst 6513); 64 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX
WS-X6416-GBIC	GBIC	16 ports; 1000BASE-SX, -LX/LH, -ZX; SC	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX
WS-X6416-GE-MT	MT-RJ	16 ports; 1000BASE-SX; MT-RJ	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX

Figure 2
Classic Gigabit Ethernet Optical Interface Modules
WS-X6416-GE-MT



6089

Cisco Catalyst CEF256 Gigabit Ethernet Optical Interface Modules

Designed for data center and server farm applications, Cisco Catalyst CEF256 optical interface modules provide line-rate Gigabit Ethernet forwarding with the following operational advantages:

Forwarding architecture—Uses the central CEF engine located on the supervisor engine

Forwarding performance—Forwards packets up to 30 Mpps per system and up to 15 Mpps per slot if upgraded to support distributed forwarding

Optics—Supports hot-pluggable GBICs

Fabric connection—Connects to the switch fabric using one 8-Gbps full-duplex connection and the 32-Gbps shared bus

Supervisor engine—Works with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—Optional; upgrade is required only to perform distributed forwarding; requir WS-F6K-DFC3 upgrade to operate with Supervisor Engine 720; requires a WS-F6K-DFC upgrade and an SFM to operate with Supervisor Engine 2-MFSC2

Slot requirements—Can occupy any slot in any Catalyst 6500 Series chassis

Port densities—192 ports: Catalyst 6513 chassis; 128 ports: Catalyst 6509 chassis

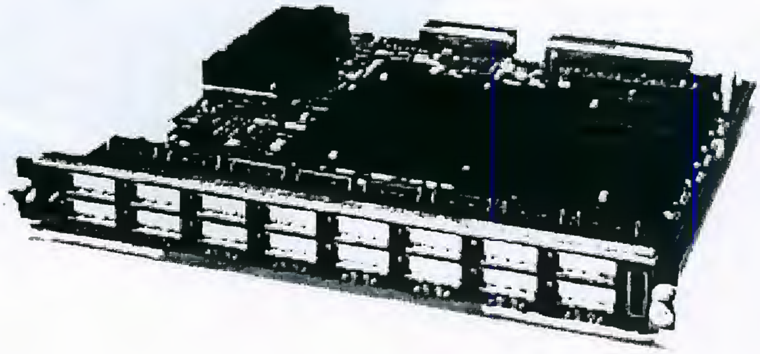
Note: Supervisor Engine 720 communicates with a CEF256 interface module in 256-Gbps mode. Supervisor Engine 720 and SFM cannot operate in the same chassis.

Table 6 CEF256 Gigabit Ethernet Optical Interface Modules

Product	Transceiver Type	Ports/Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type
WS-X6516-GBIC	GBIC	16 ports; 1000BASE-SX, -LX/LH, -ZX; SC	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX
WS-X6516A-GBIC	GBIC	16 ports; 1000BASE-SX, -LX/LH, -ZX; SC	192 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX

Figure 3

CEF256 Gigabit Ethernet Optical Interface Modules
WS-X6516A-GBIC



Cisco Catalyst dCEF256 Gigabit Ethernet Optical Interface Modules

Designed for distribution and core layers and for data-center and Web-hosting applications, Cisco Catalyst dCEF256 optical interface modules provide line-rate Gigabit Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use the dCEF engine and dCEF tables located on the interface module

Forwarding performance—Forward packets up to 24 Mpps per slot when interface modules have dual-fabric connections

Optics—Support hot-pluggable GBICs over single-mode fiber

Fabric connection—Connect using dual 8-Gbps full-duplex serial channel connections to fabric on a Supervisor Engine 720 or a SFM

Supervisor engine—Work with Supervisor Engine 2 with a SFM or Supervisor Engine 720

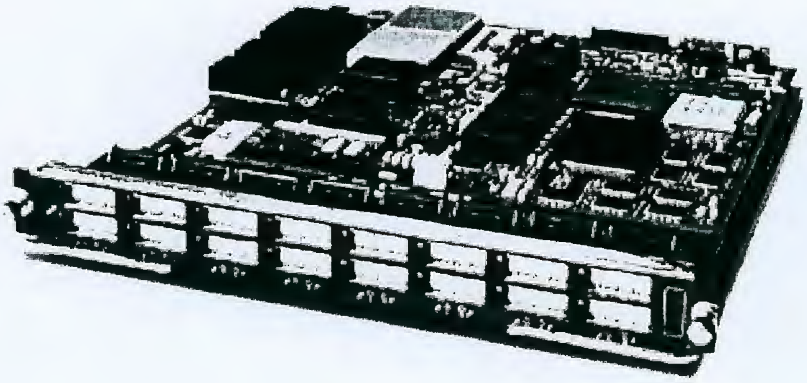
Distributed forwarding—Include a DFC when operating with Supervisor Engine 2 or a DFC3 when operating with Supervisor Engine 720

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis except the 6513 chassis where they must be installed in slots 9 through 13 (the only slots on the chassis with dual fabric connections)

Table 7 dCEF256 Gigabit Ethernet Optical Interface Modules

Product	Transceiver Type	Ports/Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type
WS-X6816-GBIC	GBIC	16 ports; 1000BASE-SX,-LX/LH, -ZX; SC	90 ports (Cisco Catalyst 6513); 128 ports (Cisco Catalyst 6509)	550 m: 1000BASE-SX 10 km: LX/LH 100 km: ZX

Figure 4
dCEF256 Gigabit Ethernet Optical Interface Modules
WS-X6816-GBIC



Interface Distances

Table 8 summarizes the interfaces and distances supported by all the Gigabit Ethernet modules in the Cisco Catalyst 6500 Series.

Table 8 Interfaces and Distances Supported by Gigabit Ethernet Modules in the Cisco Catalyst 6500 Series

Module	Interface/Fiber Core	62.5	um MM 160/500 MHz-km	62.5 um MM 200/500 MHz-km	50 um MM 400/400 MHz-km	50 um MM 500/500 MHz-km	9/10 um Single Mode	Dispersion Shifted	Category 5 UTP
WS-X6416-GE-MT	MT-RJ	220 m	275 m	500 m	550 m				
WS-X6408-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6408A-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6416-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6516-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6816-GBIC	1000BASE-SX	220 m	275 m	500 m	550 m				
WS-X6408A-GBIC	1000BASE-LX/LH	550 m	550 m	550 m	550 m		10 km		
WS-X6416-GBIC	1000BASE-LX/LH	550 m	550 m	550 m	550 m		10 km		
WS-X6516-GBIC	1000BASE-LX/LH	550 m	550 m	550 m	550 m		10 km		
WS-X6816-GBIC	1000BASE-LX/LH	550 m	550 m	550 m	550 m		10 km		
WS-X6408-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6408A-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6416-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6516-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6816-GBIC	1000BASE-ZX						70 km	100 km	
WS-X6316-GE-TX	RJ-45								100 m

6086 1
L

Ordering Information

Table 9 provides part number information for Catalyst 6500 Series chassis.

Table 9 Catalyst 6500 Series Chassis Part Numbers

Product Number	Description
WS-X6316-GE-TX	16-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches; RJ-45
WS-X6408-GBIC	8-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches; requires GBICs
WS-X6408A-GBIC	8-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches with enhanced QoS; requires GBICs
WS-X6416-GBIC	16-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches; requires GBICs
WS-X6416-GE-MT	16-port Classic Gigabit Ethernet interface module for the Cisco Catalyst 6000 Series switches; MT-RJ
WS-X6516-GBIC	16-port CEF256 Gigabit Ethernet interface module for the Cisco Catalyst 6500 Series switches with single fabric channel interface; requires GBICs; upgradable to support distributed forwarding through the addition of the distributed forwarding daughter card (WS-F6K-DFC)
WS-F6K-DFC	Distributed forwarding daughter card for CEF26 interface modules
WS-X6816-GBIC	16-port dCEF256 Gigabit Ethernet interface module for the Cisco Catalyst 6500 Series switches with dual fabric channel interfaces and distributed forwarding; requires GBICs
WS-X6816A-GBIC	16-port dCEF256 Gigabit Ethernet interface module for the Cisco Catalyst 6500 Series switches with dual fabric channel interfaces and distributed forwarding; requires GBICs
GLC-SX-MM	1000BASE-SX SFP (multimode only) Dual LC connector
GLC-SX-MM=	1000BASE-SX SFP (multimode only) spare Dual LC connector
GLC-LH-SM	1000BASE-LX SFP (single mode only) Dual LC connector
GLC-ZX-SM	1000BASE-ZX SFP (single mode only) Dual LC connector
WS-G5484	1000BASE-SX SX GBIC (multimode only)
WS-G5485	1000BASE-LX/LH LH GBIC (single mode or multimode)
WS-G5487	1000BASE-ZX ZX GBIC (single mode only)

Specifications

Standard Protocols

- IEEE 802.1d, IEEE 802.1p, IEEE 802.1q, IEEE 802.1s, IEEE 802.1w, IEEE 802.3x, IEEE 802.3z, IEEE 802.3ab, and IEEE 802.3ad,
- 1000BASE-X (GBIC), 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, CWDM

Physical Specification

- Occupies one slot in the Cisco Catalyst 6500 Series chassis
- Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)

Environmental Conditions

- Operating temperature: 32 to 104 F (0 to 40 C)
- Storage temperature: –40 to 167 F (–40 to 75 C)
- Relative humidity: 10 to 90%, noncondensing
- Operating altitude: –60 to 4000 m
- Mean time between failure (MTBF): seven years for system configuration

Safety Compliance

Cisco Catalyst 6500 Series Gigabit Ethernet interface modules, when installed in a system, comply with the following compliance and safety standards:

- UL 1950
- CSA C22.2 No.950
- EN 60950
- EN 60825-1
- IEC 60950
- IEC 60825-1
- TS 001
- CE marking
- AS/NZS 3260
- 21CFR1040

EMC Compliance

Cisco Catalyst 6500 Series Gigabit Ethernet modules, when installed in a system, comply with the following EMI standards:

- FCC Part 15 (CFR 47) Class A
- VCCI
- EN55022
- EN55024
- CISPR 22
- CE marking
- AS/NZS 3548

Network Management

- ETHERLIKE-MIB (RFC 1643)
- IF-MIB (RFC 1573)
- Bridge MIB (RFC 1493)
- CISCO-STACK-MIB
- CISCO-VTP-MIB
- CISCO-CDP-MIB

- RMON MIB (RFC 1757)
- CISCO-PAGP-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-VLAN-BRIDGE-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- ENTITY-MIB (RFC 2037)
- HC-RMON
- RFC1213-MIB (MIB-II)
- SMON-MIB

Maximum Station-to-Station Cabling Distance

- 1000BASE-SX: 62.5 um multimode fiber: up to 275 m
- 1000BASE-SX: 50 um multimode fiber: up to 550 m
- 1000BASE-LX: 62.5 um multimode fiber: up to 550 m
- 1000BASE-LX: 50 um multimode fiber: up to 550 m
- 1000BASE-LX: 9/10 um single-mode fiber: up to 5 km[1]
- 1000BASE-LH: 62.5 um multimode fiber: up to 550 m
- 1000BASE-LH: 50 um multimode fiber: up to 550 m
- 1000BASE-LH: 9/10 um single-mode fiber: up to 10 km
- 1000BASE-ZX: 9/10 um single-mode fiber: up to 70 km
- 1000BASE-ZX: disposition shifted fiber: up to 100 km
- 1000BASE-T: Category 5 cable: up to 100 m
- 10/100/1000BASE-T: Category 5 cable: up to 100 m

Indicators and Interfaces

- Status: green (operational); red (faulty); orange (module booting or running diagnostics)
- Link good: green (port active); orange (disabled); off (not active or not connected); blinking orange (failed diagnostic and disabled)
- 1000BASE-SX: GBIC (female, multimode)
- 1000BASE-LX/LH: GBIC (female, multimode)
- 1000BASE-LX/LH: GBIC (female, single mode)
- 1000BASE-ZX: GBIC (female, single mode)
- 1000BASE-ZX: GBIC (female, dispersion shifted)
- 1000BASE-SX: MT-RJ (female, multimode)
- 1000BASE-T: RJ-45
- 10/100/100BASE-T: RJ-45

[1] Cisco 1000BASE-LX/LH interfaces fully comply with the IEEE 802.3z 1000BASE-LX standard. However, their higher quality allows them to reach 10 km over single-mode fiber versus the 5 km specified in the standard.

6033

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit:
http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Additional Cisco Catalyst 6500 Series Information

Visit this link for to view the following data sheets:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 1A/Supervisor Engine 2 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Data Sheet
- Cisco Catalyst 6500 Series 10-Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series FlexWAN Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Switch Fabric Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Content Services Module (CSM) Data Sheet
- Cisco Catalyst 6500 Series Firewall Services Module Data S
- Cisco Catalyst 6500 Series Network Application Module (NAM) Data Sheet
- Cisco Catalyst 6500 Series Intrusion Detection (IDS) Module Data Sheet
- Cisco Catalyst 6500 Series IPsec/VPN Services Module Data Sheet
- Cisco Catalyst 6500 Series SSL Services Module Data Sheet

Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice EQ

Cisco Systems

Data Sheet

Cisco Catalyst 6500 Series
10/100 and 10/100/1000 **Ethernet** Interface Modules

As Cisco's premier modular multilayer switch, the Catalyst® 6500 Series delivers secure, converged services from the wiring closet to the core, to the data center, to the WAN edge.

The Cisco Catalyst® 6500 Series provides the broadest selection of 10/100 and 10/100/1000 Ethernet media, inline power options, densities, performance, interoperability, and chassis deployments. Equally suited for basic wiring closets, small campus distribution/core layers, and high performance data centers, Catalyst 6500 10/100 and 10/100/1000Mbps modules scale from 16-ports up to 576-ports in a single Catalyst 6500 chassis. Catalyst 6500 10/100 and 10/100/1000Mbps modules feature include:

- Proven and widely deployed Cisco AVVID wiring closet solution—Establish the Cisco Catalyst 6500 Series as the most widely deployed IP telephony port-enabled campus switch platform
- Choice of media and connector types—Available in copper unshielded twisted-pair (UTP), shielded twisted-pair (STP) using RJ-45 or RJ-21, multimode fiber (62.5/125 micron), and single-mode fiber using MT-RJ 100FX and 10FL
- IP phone and wireless access point support—Support inline power field upgrade (copper only), NIC/Phone auto-detection (phone discovery), and voice VLANs
- Simplified network operation with cable fault detection—Test cabling using Time Domain Reflectometer (TDR) that sends signals down the cable to identify faults in each twisted pair (available for 10/100/1000 copper
- Range of port densities—Available with 16 up to 48 ports per module; with up to 576 10/100/1000Base-TX ports, 288 ports of 100-Base-FX, or 10BASE-FL (per 13-slot chassis configured with 12 interface modules)
- Scalable and predictable performance—Provide a selection of switch fabric connections and throughput: 32 Gbps bandwidth/15 Mpps (Classic interface modules), 256 Gbps bandwidth/30 Mpps (CEF256 interface modules) and 256 Gbps bandwidth/210 Mpps(dCEF256 interface modules)
- IEEE 802.3 triple-speed autonegotiation—Allow switches to negotiate speed (10, 100, and now 1000 Mbps) and duplex mode (half or full) with attached devices
- Superior traffic management—Available with large 1-MB-per-interface buffers and up to 8 transmit queues for traffic prioritization and policing

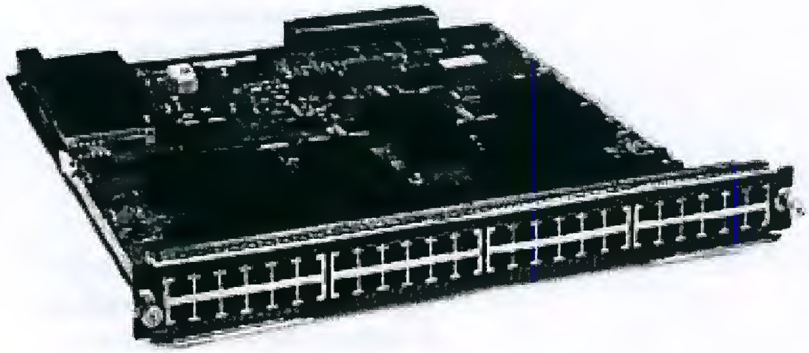
- Operational consistency—Supported in all Catalyst 6500 3-, 6-, 9-, and 13-slot chassis running Cisco IOS® Software and Cisco Catalyst Operating System Software; interoperable with all other interfaces and services modules; and forward-compatible with all Catalyst 6500 supervisor engines
- Maximum network uptime and resiliency—Support Cisco enhanced Per-Virtual LAN (VLAN) Spanning Tree Plus (PVST+) protocol, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) and IEEE 802.1s Multiple Spanning Tree (MST) protocol, Per-VLAN Rapid Spanning Tree (PVRST) protocol, Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Cisco EtherChannel®, and IEEE 802.3ad link aggregation for fault-tolerant connectivity
- Extensive management tools—Support CiscoWorks network management platform; Simple Network Management Protocol (SNMP) versions 1, 2, and 3; and four Remote Monitoring (RMON) groups (statistics, history, alarms, and events)

The newest members of the Cisco Catalyst 6500 Series 10/100/1000 product family—the Classic interface module WS-X6148-GE-TX and the CEF256 interface module WS-X6548-GE-TX—provide 10/100/1000 Gigabit netwo access using standard RJ-45 connectors (Figure 1).

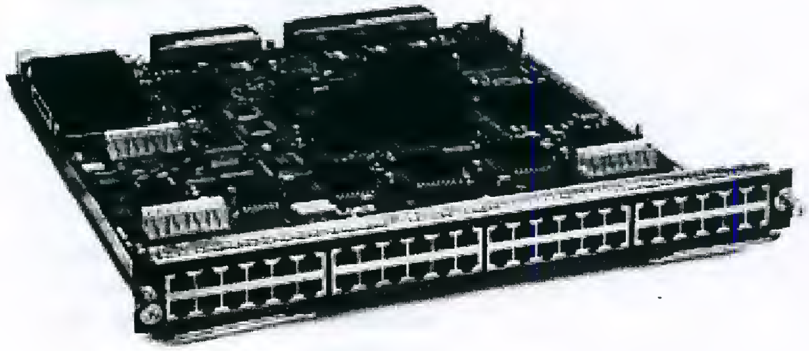
Figure 1

Cisco Catalyst 6500 Series 48-Port RJ-45 10/100/1000 Ethernet Interface Modules

WS-X6148-GE-TX



WS-X6548-GE-TX



Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Applications

Ethernet and Fast Ethernet 10/100 and 10/100/1000 interface modules are used in both wiring closet and data center applications (Figure 2; Table 1).

Table 1 Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Copper Interface Module Applications

Primary Applications	Product Number	Interface Module Class	Ports/ Connector/ Interface	Inline Power Support[1]	Queues per Port (Tx = Transmit, Rx = Receive)[2]	Buffer Size
Data Center and Server Farm	WS-X6516-GE-TX	CEF256	16, RJ-45, 10/100/1000	No	Tx–1p2q2T, Rx–1p1q4T	512 KB per port
Server Farm	WS-X6548-RJ-45	CEF256	48, RJ-45, 10/100	No	Tx–1p3q1t, Rx–1p1q0t	1 MB per port
Server Farm	WS-X6548-RJ-21	CEF256	48, RJ-21, 10/100	No	Tx–1p3q1t, Rx–1p1q0t	1 MB per port
Premier Wiring Closet	WS-X6548V-GE-TX	CEF256, Not Upgradable to dCEF	48, RJ-45, 10/100/1000	Both	Tx–1p2q2t (per 8 ports), Rx–1p2t (per port)	1 MB per 8 ports
Premier Wiring Closet	WS-X6548-GE-TX	CEF256, Not Upgradable to dCEF	48, RJ-45, 10/100/1000	Both, Upgr	Tx–1p3q1t, Rx–1p1q4t	1 MB per 8 ports
Wiring Closet	WS-X6148V-GE-TX	Classic	48, RJ-45, 10/100/1000	Both	Tx–1p2q2t, Rx–1q2t	1 MB per 8 ports
Wiring Closet	WS-X6148-GE-TX	Classic	48, RJ-45, 10/100/1000	Both, Upgr	Tx–1p2q2t, Rx–1q2t	1 MB per 8 ports
Base Wiring Closet	WS-X6148-RJ45V	Classic	48, RJ-45, 10/100/1000	Both	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6148-RJ21V	Classic	48, RJ-21, 10/100	Both	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6148-RJ-45	Classic	48, RJ-45, 10/100	Both, Upgr	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6148-RJ-21	Classic	48, RJ-21, 10/100	Both, Upgr	Tx–2q2t, Rx–1q4t	128 KB per port
Base Wiring Closet	WS-X6348-RJ45V	Classic	48, RJ-45, 10/100	Cisco	Tx 2q2t, Rx 1q4t	128 KB per port
Base Wiring Closet	WS-X6348-RJ21V	Classic	48, RJ-21, 10/100	Cisco	Tx 2q2t, Rx 1q4t	128 KB per port

[1] **Inline Power Legend:**
Both = Cisco inline power (available now) and IEEE 802.3af (via future field upgradable daughter card)
Cisco = Cisco inline power only
Upgr = shipped as data only but upgradable to the inline power type specified
No = inline power not supported

[2] **Queues Legend:** 1p7q8t = 1 priority queue, 7 round robin queues, 8 thresholds

Table 2 Cisco Catalyst 6500 Series 100FX and 10FL Fiber Interface Module Applications

Primary Applications	Product Number	Interface Module Class	Ports/ Connectors/ Interface Media	Queues per Port (Tx = Transmit, Rx = Receive)[1]	Buffers
Access, Server Farm	WS-X6524-100FX-MM	CEF256, Upgradable to dCEF	24, MM MT-RJ, 100FX	Tx 1p3q1t, Rx 1p1q0t	1 MB per port
Access, Server Farm	WS-X6324-100FX-MM	Classic	24, MM, MT-RJ, 100FX	Tx 2q2t, Rx 1q4t	128 KB per port
Access, Server Farm	WS-X6324-100FX-SM	Classic	24, SM MT-RJ, 100FX	Tx 2q2t, Rx 1q4t	128 KB per port
Access	WS-X6024-10FL-MT	Classic	24, MM MT-RJ, 10FL	Tx 2q2t, Rx 1q4t	64 KB per port

[1] **Queues Legend:** 1p3q1t = 1 priority queue, 3 round robin queues, 1 threshold

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet Interface Modules with Cisco Inline Power

The Cisco Catalyst 6500 Series delivered the first 10/100BASE-T Ethernet switching modules that provided inline power for converged data and voice traffic. Cisco Catalyst Classic interface modules support voice functionality on each interface port, allowing customers to build campus multiservice data and voice networks for wiring closets with the following features:

- Inline power—Provides 48-volt DC power (for Cisco Inline Power and IEEE 802.3af standard inline power when it becomes available) over standard Category 5 unshielded twisted-pair (UTP) cable up to 100 meters for IP phones and wireless access points
- Phone discovery—Detects the presence of an IP phone and supplies inline power automatically
- Auxiliary VLAN using 802.1Q—Segments IP phones and data endpoints into separate logical networks automatically
- AutoQoS

Cisco Catalyst Inline Power and IEEE 802.3af Inline Power

The Inline Power feature gives network administrators centralized power control. It works over existing Category 5 UTP installations and helps to ensure that building power outages will not affect network telephony connections, providing greater network availability—when Cisco Catalyst 6500 Series switches are configured with uninterruptible power supply (UPS) systems.

10/100 and 10/100/1000 Ethernet interface modules shipping today support the Cisco Inline Power feature or support the IEEE 802.3af standard, or both, allowing 802.3af capability to be added later through an upgrade. The Cisco Catalyst Inline Power feature implementation passes the required domestic and international safety regulations and compliance measures.

Phone Discovery

The Cisco phone discovery feature eases network management burdens by automating the Inline Power feature. With phone discovery, the Cisco Catalyst switch detects the presence of an IP phone and supplies inline power automatically, eliminating the need to manually enable ports for inline power. The phone discovery mechanism is intelligent enough to differentiate between an IP phone and a network interface card (NIC), and will not supply inline power to NICs or other devices not designed to use inline power. With this feature, network administrators can depend on automatic and centralized control of inline power that is safe to deploy and maintain.

Auxiliary VLAN

The unique Auxiliary VLAN feature offered by Cisco provides automatic VLAN configuration for IP phones. It places phones into their own VLANs automatically, simplifying the task of overlaying a voice topology onto a data network. It allows network administrators to easily segment phones into separate logical networks, even though the data and voice infrastructure is physically the same—greatly simplifying the task of managing a multiservice network and identifying and troubleshooting network problems.

The Auxiliary VLAN feature maintains VLAN assignments, even when phones are moved to new locations. When a user plugs a phone into the switch, the switch provides the phone with the necessary VLAN information.

AutoQoS

Network administrators can assign IP phones to separate IP subnets and VLANs to allow separate quality of service (QoS) or security policies for IP phones. By deploying AutoQoS that configures QoS on voice ports automatically, the administrative task of configuring QoS to establish end-to-end traffic prioritization is greatly simplified.

Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Modules

Two classes of Cisco Catalyst 6500 Series 10/100 and 10/100/1000 Ethernet interface modules—Classic and CEF256—provide a choice of speeds and forwarding rates (Table 4).

Classic 10/100 and 10/100/1000 Interface Modules

Suited for wiring closet applications, Classic 10/100 and 10/100/1000 modules use the supervisor's centralized forwarding engine for Layer 3 forwarding, and forward packets up to 15 Mpps.

Capable of operating in the same chassis with Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, Classic Series modules do not support distributed forwarding and cannot be upgraded with a Distributed Forwarding Card (DFC).

CEF256 10/100 and 10/100/1000 Interface Modules

Suited for premier wiring closet, distribution and core layers, data-center, and Web-hosting applications, CEF256 10/100 and 10/100/1000 interface modules use the centralized CEF engine located on the supervisor engine's policy feature card (PFC) and forward packets up to 30 Mpps.

Capable of operating in the same chassis with Supervisor Engine 1A, Supervisor Engine 2, and Supervisor Engine 720, CEF256 interface modules can also support distributed forwarding (Table 2).

Table 3 CEF256 10/100 and 10/100/1000 Switch Fabric DFC Upgrade Requirements

Supervisor Engine	Switch Fabric	DFC
Supervisor Engine 2 MSFC2/PFC2	Separate switch fabric module (SFM)	Requires WS-F6K-DFC upgrade
Supervisor Engine 720	Supervisor Engine 720 contains a switch fabric	Requires WS-F6K-DFC3 upgrade; will not work with WS-F6K-DFC3, or WS-F6K-DFC

Table 4 provides a comparison of the interface module classes available for 10/100 and 10/100/1000 Ethernet interface modules.

Table 4 Classic and CEF256 10/100 and 10/100/1000 Interface Module Comparison

Feature	Classic Interface Modules	CEF256 Interface Modules
Performance/ Forwarding Rate (Mpps)	32 Gbps; 15 Mpps per system	256 Gbps; Up to 30 Mpps per system (15 Mpps per slot for slots upgraded with DFC to support distributed forwarding)
Forwarding Engine Architecture	Supervisor engine CPU makes forwarding decision	Centralized CEF engine located on supervisor's PFCx daughter card makes forwarding decision upgradeable to dCEF switching with optional WS-F6K-DFC or WS-F6K-DFC3
Supervisor Engine Supported	Supervisor Engine 1A, Supervisor Engine 2, Supervisor Engine 720	Supervisor Engine 1A, Supervisor Engine 2, Supervisor Engine 720
DFC Upgrade Requirements	Not supported	None integrated; Supervisor Engine 2—WS-F6K-DFC upgrade; SupervisorEngine 720—WS-F6K-DFC3 upgrade
Fabric Connections	32 Gbps shared bus connection (on Supervisor Engine1A, Supervisor Engine 2, and Supervisor Engine 720)	Single 8-Gbps channel connection to switch fabric [on Supervisor Engine 720 or Supervisor Engine 2-MSFC2 with Switch Fabric Module (SFM)] and 32-Gbps shared bus connection
Slot Requirements	Can occupy any slot in any chassis	Can occupy any slot in any chassis
Scheduler	Weighted Round Robin (WRR)	WRR

6075

Cisco Catalyst Classic 10/100/1000 Voice Interface Modules

Suited for wiring closet applications, Cisco Catalyst Classic 10/100/1000 voice interface modules (Table 5) provide access to the desktop through standard RJ-45 connectors with the following operational advantages:

Forwarding architecture—Centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Fabric connection—Provide a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Time Domain Reflectometer (TDR)—Tests cabling by sending signals down the cable to identify faults in each twisted pair

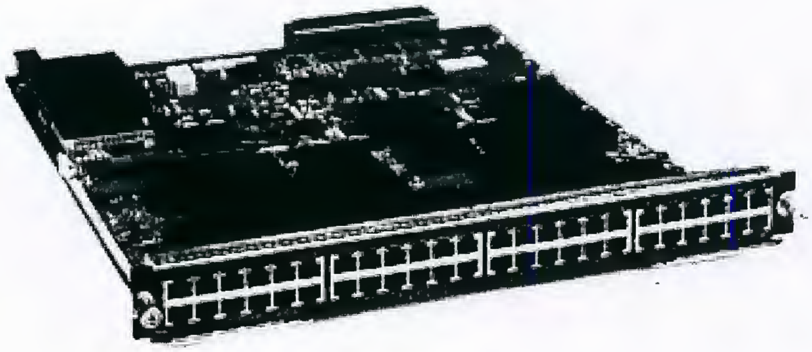
Transmit queue structure—1p2q2t = 1 strict priority queue, 2 round robin queues, 2 thresholds

Receive queue structure—1q2t = 1 round robin queue, 2 thresholds

Table 5 Classic 10/100/1000 Voice Interface Modules

Product	Ports/ Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type	Inline Power for Voice Availability/ Upgrade Capability
WS-X6148-GE-TX	48-port;10/100/ 1000BASE-TX; RJ-45	576 ports (Cisco Catalyst 6513); 384 ports (Cisco Catalyst 6509)	100 meters; Category 5 cable	Cisco Inline Power; upgradable to 802.3af
WS-X6148V-GE-TX	48-port; 10/100/ 1000BASE-TX; RJ-45	576 ports (Cisco Catalyst 6513); 384 ports (Cisco Catalyst 6509)	100 meters; Category 5 cable	Cisco Inline Power; upgradable to 802.3af

Figure 2
Classic 10/100/1000 Voice Interface Modules
WS-X6148V-GE-TX



Cisco Catalyst CEF256 10/100/1000 Voice Interface Modules

Suited for wiring closet applications, Cisco Catalyst CEF256 10/100/1000 voice interface modules provide access to the desktop through standard RJ-45 connectors and line-rate 10/100/1000 Ethernet forwarding (Table 6) with the following operational advantages:

Forwarding architecture—Use the central CEF engine located on the supervisor engine

Forwarding performance—Forward packets up to 30 Mpps per system and up to 15 Mpps per slot if upgraded to support distributed forwarding

Fabric connection—Connect to the switch fabric through one 8-Gbps connection and the 32-Gbps shared bus

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine720

Distributed forwarding upgrade—Optional; upgrade is required only to perform distributed forwarding; requires a WS-F6K-DFC3 upgrade to operate with a Supervisor Engine 720; requires a WS-F6K-DFC upgrade to operate with a Supervisor Engine2/MFSC2 and a Switch Fabric Module

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Time Domain Reflectometer (TDR)—Tests cabling by sending signals down the cable to identify faults in each twisted pair

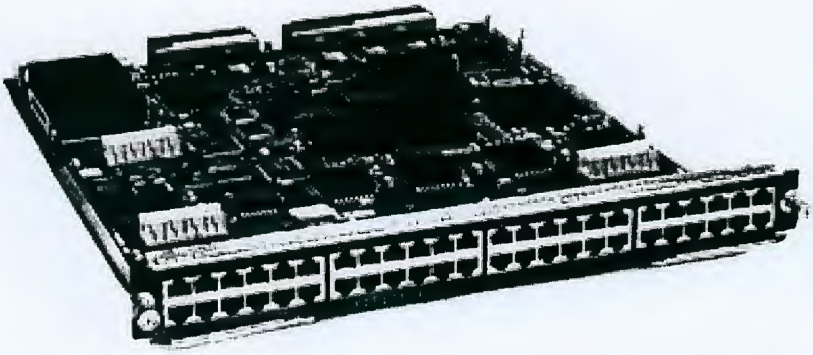
Transmit queue structure—1p2q2t = 1 priority queue, 2 round robin queues, 1 threshold

Receive queue structure—1q2t = 1 round robin queue, 2 thresholds

Table 6 CEF256 10/100/1000 Voice Interface Modules

Product	Ports/ Interface/ Connectors	Port Density/ Chassis Model	Maximum Distance/ Cable Type	Inline Power for Voice Availability/ Upgrade Capability
WS-X6548-GE-TX	48-port; 10/100/1000BASE-TX; RJ-45	576 ports (Cisco Catalyst 6513); 384 ports (Cisco Catalyst 6509)	100 meters; Category 5 cable	Cisco Inline Power; upgradable to 802.3af

Figure 3
CEF256 10/100/1000 Voice Interface Modules
WS-X6548-GE-TX



Cisco Catalyst Classic 10/100 Copper Voice Modules

Designed for deployment in wiring closets, high-density Cisco Catalyst Classic 10/100 interface modules come with a selection of inline power capabilities and provide line-rate 10/100 Ethernet forwarding with the following operational advantages:

- Voice-ready modules with Cisco Inline Power and upgradable to 802.3af—Available in 48-port RJ-45 and RJ-21 configurations (WS-X6148-RJ45V and WS-X6148-RJ21V)
- Voice-ready modules with Cisco Inline Power and not upgradable to 802.3af—Available in 48-port RJ-45 and RJ-21 configurations (WS-X6348-RJ45V and WS-X6348-RJ21V)
- Voice-capable modules upgradable to Cisco Inline Power or 802.3af—Available in 48-port RJ-45 and RJ-21configurations (WS-X6148-RJ-45 and WS-X6148-RJ-21)

Note: These modules are designed to fully support future upgrades to the IEEE 802.3af inline power standard currently underway, providing maximum investment protection.

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forwards packets up to 15 Mpps per system

Fabric connection—Connect to the switch fabric using a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Transmit queue structure—2q2t = two round robin queues and two thresholds

Receive queue structure—1q4t = one round robin queue and four thresholds

Table 7 Classic 10/100 Copper Voice Interface Modules

Product	Ports/ Interface/ Connectors	Port Density/ Chassis Model/	Maximum Distance/Cable Type	Inline Power for Voice Availability/ Capability

WS-X6148-RJ45	48-port;
	10/100BASE-TX;
	RJ-45
		576 ports
		(Cisco Catalyst 6513);
		384 ports
		(Cisco Catalyst 6509)
			100 meters;
			Category 5 cable
				Cisco Inline Power;
				upgradable to 802.3af

WS-X6148-RJ21V	48-port;
	10/100BASE-TX;
	RJ-21
		576 ports
		(Cisco Catalyst 6513);
		384 ports
		(Cisco Catalyst 6509)
			100 meters;
			Category 5 cable
				Cisco Inline Power;
				upgradable to 802.3af

WS-X6348-RJ45V	48-port;
	10/100BASE-TX;
	RJ-45
		576 ports
		(Cisco Catalyst 6513);
		384 ports
		(Cisco Catalyst 6509)
			100 meters;
			Category 5 cable
				Cisco Inline Power;
				cannot upgrade to
				802.3af

WS-X6348-RJ21V	48-port;
	10/100BASE-TX;
	RJ-21
		576 ports
		(Cisco Catalyst 6513);
		384 ports
		(Cisco Catalyst 6509)
			100 meters;
			Category 5 cable
				Cisco Inline Power;
				cannot upgrade to
				802.3af

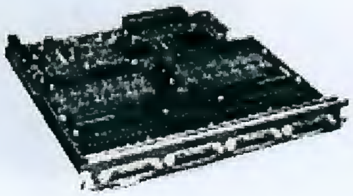
WS-X6148-RJ-45	48-port;
	10/100BASE-TX;
	RJ-45
		576 ports
		(Cisco Catalyst 6513);
		384 ports
		(Cisco Catalyst 6509)
			100 meters;
			Category 5 cable
				None provided; can
				upgrade to Cisco Inline
				Power or 802.3af

WS-X6148-RJ-21	48-port;
	10/100BASE-TX;
	RJ-21
		576 ports
		(Cisco Catalyst 6513);
		384 ports
		(Cisco Catalyst 6509)
			100 meters;
			Category 5 cable
				None provided; can
				upgrade to Cisco Inline
				Power or 802.3af

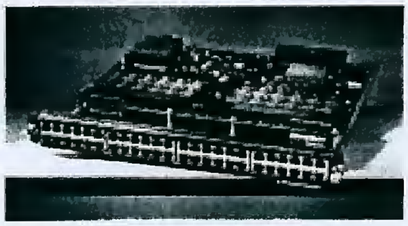
Figure 4

Classic 10/100 Copper Voice Interface Modules

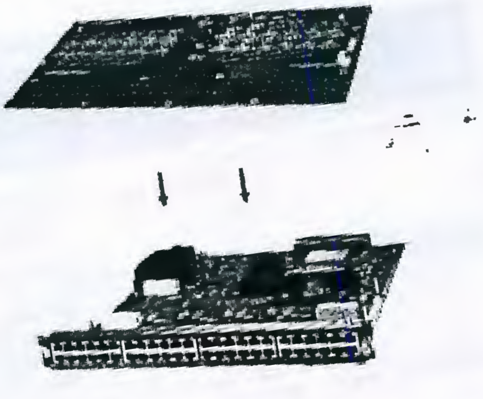
WS-X6148-RJ45



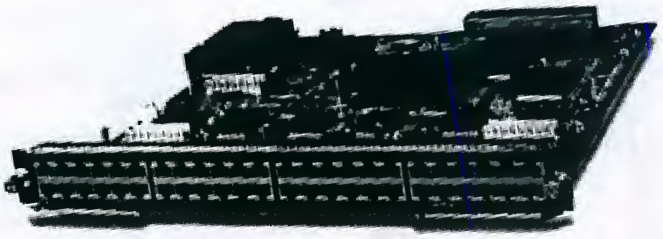
VWS-X6148-RJ21V



WS-X6348-RJ21V



WS-X6148-RJ-45



WS-X6148-RJ-21

Cisco Catalyst CEF256 10/100 Copper Modules

Designed for small campus distribution and core layers and for data-center and Web-hosting applications where voice capability is not required, Cisco Catalyst CEF256 twisted-pair interface modules provide line-rate 10/100 Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use the central CEF engine located on the supervisor engine

Forwarding performance—Forward packets up to 30 Mpps per system and up to 15 Mpps per slot for slots upgraded to support distributed forwarding

Fabric connection—Connect to the switch fabric using a single 8-Gbps switch fabric channel and a 32-Gbps shared bus

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—Only required to perform distributed forwarding; require a WS-F6K-DFC3 upgrade to operate with Supervisor Engine 720; require a WS-F6K-DFC upgrade to operate with Supervisor Engine 2/ MFSC2 and an SFM

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Transmit queue structure—1p3q1t = 1 priority queue, 3 round robin queues, 1 threshold

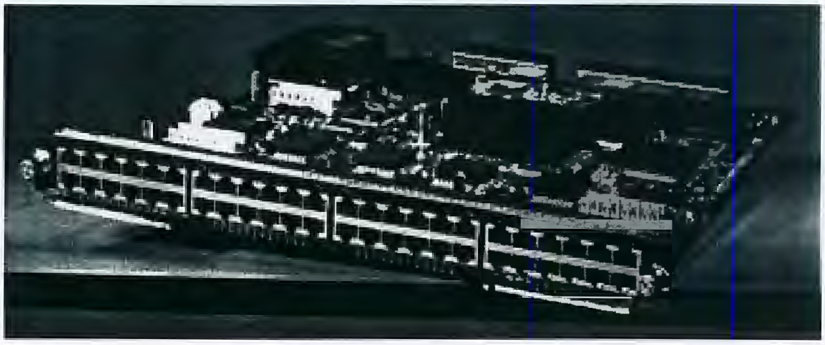
Receive queue structure—1p1q4t = 1 priority queue, 1 round robin queue, 4 thresholds

Table 8 CEF256 Copper 10/100 Interface Modules

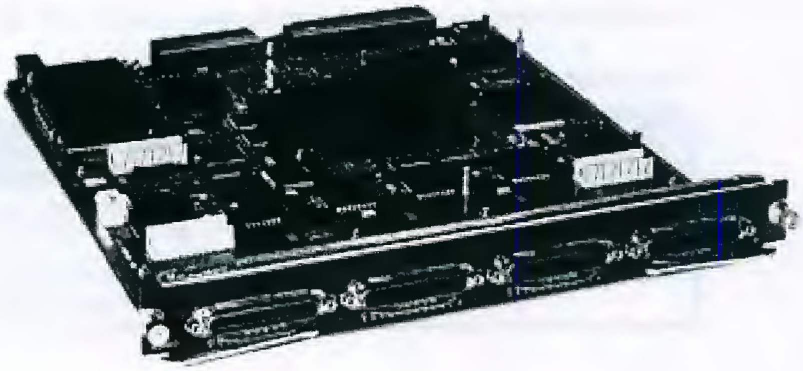
Product	Ports/Interface/ Connectors	Port Density/Chassis Model	Maximum Distance/ Cable Type
WS-X6548-RJ-45	48-port; 10/100BASE-TX; RJ-45	576 ports (Cisco Catalyst 6513); 384 ports (Cisco Catalyst 6509)	100 meters; Category 5 cable
WS-X6548-RJ-21	48-port; 10/100BASE-TX; RJ-21	576 ports (Cisco Catalyst 6513); 384 ports (Cisco Catalyst 6509)	100 meters; Category 5 cable

Figure 5 shows high-density Cisco Catalyst CEF256 copper interface modules designed for distribution and core layers.

Figure 5
CEF256 Copper 10/100 Interface Modules
WS-X6548-RJ-45



WS-X6548-RJ-21



Catalyst Classic 100FX and 10FL Fiber Interface Modules

Designed for deployment in wiring closets where optical interfaces are required, the Cisco Catalyst Classic fiber interface modules provide 10/100 Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use centralized CEF forwarding

Forwarding performance—Forward packets up to 15 Mpps per system

Fabric connection—Connect to the switch fabric using a 32-Gbps shared bus connection

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—None; Classic interface modules cannot be upgraded for distributed forwarding

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Transmit queue structure—2q2t = 2 round robin queues, 2 thresholds

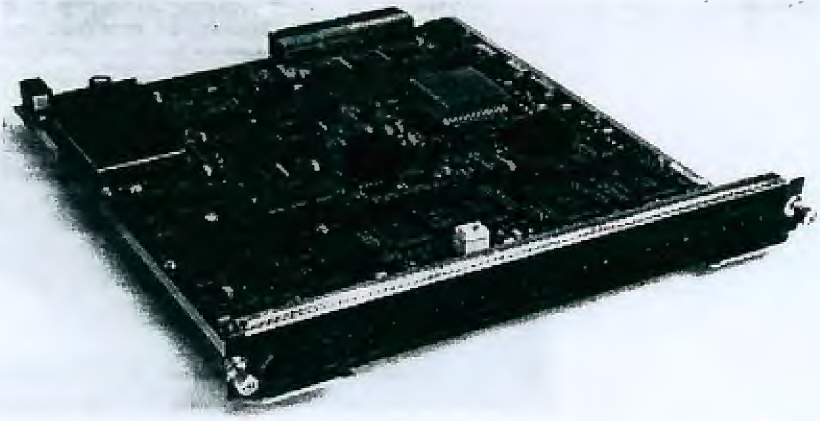
Receive queue structure—1q4t = 1 round robin queue, 4 thresholds

Note: No inline power support for voice is available for 100FX/10FL fiber modules.

Table 9 Classic 100FX/10FL Fiber Interface Modules

Product	Ports/ Interface/ Connectors	Port Density/Chassis Model	Maximum Distance/Cable Type
WS-X6324-100FX-MM	24-port; 100BASE-FX; MT-RJ	288 ports (Cisco Catalyst 6513); 192 ports (Cisco Catalyst 6509)	2 km; –62.5/125-micron multimode fiber; full or half duplex
WS-X6324-100FX-SM	24-port; 100BASE-FX; MT-RJ	288 ports (Cisco Catalyst 6513); 192 ports (Cisco Catalyst 6509)	2 km; –62.5/125-micron multimode fiber; full or half duplex
WS-X6024-10FL-MT	24-port; 10FL; MT-RJ	288 ports (Cisco Catalyst 6513); 192 ports (Cisco Catalyst 6509)	2 km; –62.5/125-micron multimode fiber; full or half duplex

Figure 6
Classic 100FX/10FLFiber Interface Modules
WS-X6024-10FL-MT



Cisco Catalyst CEF256 100FX Fiber Modules

Designed for small campus distribution and core layers and for data-center and Web-hosting applications, Cisco Catalyst dCEF256 fiber interface modules provide line-rate 100FX Ethernet forwarding with the following operational advantages:

Forwarding architecture—Use the central CEF engine located on the supervisor engine

Forwarding performance—Forward packets up to 30 Mpps per system and up to 15 Mpps per slot for slots upgraded to support distributed forwarding

Fabric connection—Connect to the switch fabric using one 8-Gbps connection and the 32-Gbps shared bus

Supervisor engine—Work with Supervisor Engine 1A, Supervisor Engine 2, or Supervisor Engine 720

Distributed forwarding upgrade—Only required to perform distributed forwarding; require a WS-F6K-DFC3 upgrade to operate with Supervisor Engine 720; require a WS-F6K-DFC upgrade to operate with Supervisor Eng 2/MFSC2 and a Switch Fabric Module

Slot requirements—Can occupy any slot in any Cisco Catalyst 6500 Series chassis

Transmit queue structure—1p3q1t = 1 priority queue, 3 round robin queues, 1 threshold

Receive queue structure—1p1q2t = 1 priority queue, 1 round robin queue, 2 thresholds

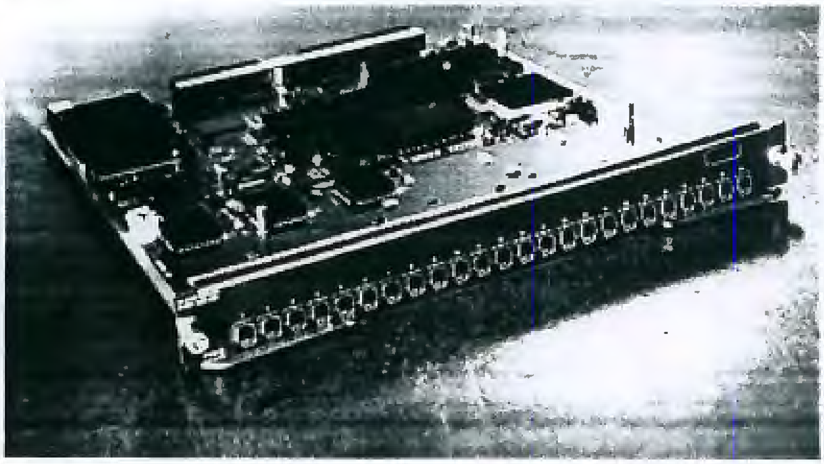
Note: No inline power support for voice is available for 100FX fiber modules.

Table 10 CEF256 100FX Fiber Interface Modules

Product	Ports/Interface/ Connectors	Port Density/Chassis Model	Maximum Distance/Cable Type

WS-X6524-100FX-MM	24-port;
	100BASE-FX;
	MT- RJ
		288 ports (Cisco Catalyst 6513);
		192 ports (Cisco Catalyst 6509)
			2 km; –62.5/125-micron multimode fiber; full or half duplex

Figure 7
CEF256 100FX Fiber Interface Modules
WS-X6524-100FX-MM



Ordering Information

Table 11 provides part number information for Catalyst 6500 Series 10/100 and 100/1000 Ethernet interface modules.

Table 11 Catalyst 6500 Series 10/100 and 100/1000 Ethernet Interface Modules

Product Number	Description
WS-X6024-10FL-MT	Catalyst 6500 24-port 10FL Classic interface module, multimode fiber, MT-RJ
WS-X6148-GE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 Classic interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-VGE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 Classic interface module; with Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-RJ-21	Catalyst 6500 48-port 10/100 RJ-21 Classic interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-RJ21V	Catalyst 6500 48-port 10/100 Telco RJ-21 Classic interface module with Cisco Inline Power
WS-X6148-RJ-45	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module; field-upgradable to support Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6148-RJ45V	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module with Cisco Inline Power
WS-X6348-RJ21V	Catalyst 6500 48-port 10/100 Telco RJ-21 Classic interface module with Cisco Inline Power
WS-X6348-RJ45	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module; field-upgradable to provide Cisco Inline Power through voice daughter card (WS-F6K-VPWR=)
WS-X6348-RJ45V	Catalyst 6500 48-port 10/100 RJ-45 Classic interface module with Cisco Inline Power
WS-F6K-VPWR=	Inline power daughter card to support Cisco Inline Power for Cisco Catalyst 6500 Series switches
WS-X6324-100FX-MM	Catalyst 6500 24-port 100FX Classic interface module, multimode fiber, MT-RJ
WS-X6324-100FX-SM	Catalyst 6500 24-port, 100FX Classic interface module, single-mode fiber, MT-RJ, with enhanced QoS
WS-X6548-RJ-45	Catalyst 6500 48-port, CEF256 10/100 RJ-45 interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)
WS-X6548-RJ-21	Catalyst 6500 48-port, CEF256 10/100 RJ-21 interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)
WS-X6524-100FX-MM	Catalyst 6500 24-port, CEF256 100FX interface module; field-upgradable to support distributed forwarding with the addition of the Distributed Forwarding daughter card (WS-F6K-DFC= or DFC3)
WS-F6K-DFC=	Distributed forwarding daughter card for interface modules running with Supervisor Engine 2 and a Switch Fabric Module
WS-F6K-DFC3=	Distributed forwarding daughter card for CEF256, dCEF256, and dCEF720 interface modules running with Supervisor Engine 720

Ordering Information—DFC Daughter Cards

Table 12 provides part number information for Catalyst 6500 Series 10/100 and 100/1000 Ethernet interface modules.

Table 12 *Catalyst 6500 Series 10/100 and 100/1000* Distributed Forwarding Cards

Part Number	Description
WS-F6K-DFC	Distributed forwarding card
WS-F6K-DFC=	Distributed forwarding card, spare
MEM-DFC-256MB	256-MB DRAM option for DFC
MEM-DFC-256MB=	256-MB DRAM spare option for DFC
MEM-DFC-512MB	512-MB DRAM option for DFC
MEM-DFC-512MB=	512-MB DRAM spare option for DFC

Specifications

Standard Network Protocols

- Ethernet: IEEE 802.3, 10BASE-T
- Fast Ethernet: IEEE 802.3, 100BASE-TX, and 100BASE-FX
- Gigabit Ethernet: 1000BASE-TX
- IEEE 802.1d, IEEE 802.1p, IEEE 802.1q, IEEE 802.1s, IEEE 802.1w, IEEE 802.3x, IEEE 802.3z, IEEE 802.3ab, IEEE 802.3ad

Physical Specification

- Occupies one slot in a Cisco Catalyst 6500 Series chassis
- Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)

Environmental Conditions

- Operating temperature: 32 to 104 F (0 to 40 C)
- Storage temperature: –40 to 167 F (–40 to 75 C)
- Relative humidity: 10 to 90%, noncondensing
- Operating altitude: –60 to 4000 m

Safety Compliance

- UL 1950
- CSA-C22.2 No. 950
- EN 60950
- IEC 950
- AS/NZS 3260
- IEC 825

- EN 60825
- 21CFR1040

EMC Compliance

- FCC Part 15 (CFR 47) Class A
- VCCI Class A with UTP, Class B with STP
- EN55022 Class A with UTP, Class B with STP
- CISPR 22 Class A with UTP, Class B with STP
- CE marking
- AS/NZS 3548 Class A with UTP, Class B with STP

Network Management

- ETHERLIKE-MIB (RFC 1643)
- IF-MIB (RFC 1573)
- Bridge MIB (RFC 1493)
- CISCO-STACK-MIB
- CISCO-VTP-MIB
- CISCO-CDP-MIB
- RMON MIB (RFC 1757)
- CISCO-PAGP-MIB
- CISCO-STP-Extensions-MIB
- CISCO-VLAN-Bridge-MIB
- CISCO-VLAN-Membership-MIB
- CISCO-UDLDP-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-COPS-CLIENT-MIB
- ENTITY-MIB (RFC 2037)
- HC-RMON
- RFC1213-MIB (MIB-II)
- SMON-MIB

Inline Power Specifications

- Output power per port: 48V DC power
- Pin assignment: 1, 2, 3, 6

Maximum Station-to-Station Cabling Distance

- 10/100BASE-TX, 100BASE-TX Fast Ethernet, and 10/100/1000: Category 5, 5e, and 6 UTP: 328 ft. (100 m), 100-ohm STP: 328 ft. (100 m); half or full duplex
- 100BASE-FX Fast Ethernet: 62.5/125-micron multimode fiber: 400-m half duplex, 2-km half or full duplex

- 100BASE-FX Fast Ethernet: 8/125-micron single-mode fiber: 10-km half or full duplex
- 10BASE-FL Ethernet: 62.5/125-micron multimode fiber: 2-km half or full duplex
- Maximum power: off (maximum power condition not reached); on (maximum power condition reached; no more phones will receive inline power from this module)

Indicators and Interfaces

- Status: green (operational); red (faulty); orange (module booting or running diagnostics)
- Link good: green (port active); orange (disabled); off (not active or not connected); blinking orange (failed diagnostic and disabled)
- 10/100/1000: RJ-45 (female)
- 10/100BASE-TX and 100BASE-TX: RJ-45 (female)
- 100BASE-FX: MT-RJ (female, multimode)
- 100BASE-FX: MT-RJ (female, single mode)
- 10BASE-FL: MT-RJ (female, multimode)

Cisco Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco is committed to maximizing the return on your network investment. Cisco offers a portfolio of technical support services to help ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

The Cisco Technical Support Services organization offers the following features, providing network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement

Cisco Technical Support Services include:

- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information, visit:

http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

Additional Cisco Catalyst 6500 Series Information

Visit this link for to view the following data sheets:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Cisco Catalyst 6500 Series Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 1A and Supervisor Engine 2 Data Sheet
- Cisco Catalyst 6500 Series Supervisor Engine 720 Data Sheet
- Cisco Catalyst 6500 Series Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series 10 Gigabit Ethernet Interface Modules Data Sheet
- Cisco Catalyst 6500 Series FlexWAN Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Switch Fabric Interface Modules Data Sheet
- Cisco Catalyst 6500 Series Content Services Module (CSM) Data Sheet
- Cisco Catalyst 6500 Series Firewall Services Module Data Sheet
- Cisco Catalyst 6500 Series Network Application Module (NAM) Data Sheet
- Cisco Catalyst 6500 Series Intrusion Detection (IDS) Module Data Sheet
- Cisco Catalyst 6500 Series IPSec/VPN Services Module Data Sheet
- Cisco Catalyst 6500 Series SSL Services Module Data Sheet

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice ER

CHAPTER 6

Configuring EtherChannel

This chapter describes how to use the command-line interface (CLI) to configure EtherChannel on the Catalyst 6500 series switches. The configuration tasks in this chapter apply to Ethernet, Fast Ethernet, and Gigabit Ethernet switching modules and the uplink ports on the supervisor engine.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Command Reference* publication.

This chapter consists of these sections:

Note You can use the commands in the following sections on all Ethernet ports in the Catalyst 6500 series switches.

Understanding How EtherChannel Works

EtherChannel aggregates the bandwidth of up to eight compatibly configured ports into a single logical link. A Catalyst 6500 series switch supports a maximum of 128 EtherChannels. All Ethernet ports on all modules, including those on a standby supervisor engine, support EtherChannel with no requirement that ports be contiguous or on the same module. All ports in each EtherChannel must be the same speed.

Note With software releases 6.3(1) and later, due to the port ID handling by the spanning tree feature, the maximum supported number of EtherChannels is 126 for a 6- or 9-slot chassis and 63 for a 13-slot chassis.

Note The network device to which a Catalyst 6500 series switch is connected may impose its own limits on the number of ports in an EtherChannel.

If a link within an EtherChannel fails, traffic previously carried over the failed link switches to the remaining links within the EtherChannel. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

You can configure EtherChannels as trunks. After a channel is formed, configuring any port in the channel as a trunk applies the configuration to all ports in the channel. Identically configured trunk ports can be configured as an EtherChannel.

Understanding EtherChannel Frame Distribution

EtherChannel distributes frames across the links in a channel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel.

EtherChannel frame distribution is based on a Cisco-proprietary hashing algorithm. The algorithm is deterministic; given the same addresses and session information, you always hash to the same port in the channel, preventing out-of-order packet delivery.

The address may be a source, a destination, or a combination of two IP addresses, two MAC addresses, or two TCP/UDP port numbers depending on the policy adopted through the **ip**, **mac**, or **session** options of the **set port channel all distribution** command. See the "Configuring EtherChannel Load Balancing" section on page 6-11 for detailed information.

Note The **set port channel all distribution session** command is supported on Supervisor Engine 2 only.

EtherChannel frame distribution is not configurable on all supervisor engines. Enter the **show module** command on a supervisor engine to determine if EtherChannel frame distribution is configurable on your switch. If the display shows the "Sub-Type" to be "L2 Switching Engine I WS-F6020," then EtherChannel frame distribution is not configurable on your Catalyst 6500 series switch; the switch uses source and destination Media Access Control (MAC) addresses.

EtherChannel frame distribution is configurable with all other switching engines. The default is to use source and destination IP addresses.

Port Aggregation Control Protocol and Link Aggregation Control Protocol

Port Aggregation Control Protocol (PAgP) and Link Aggregation Control Protocol (LACP) are two different protocols that allow ports with similar characteristics to form a channel through dynamic negotiation with adjoining switches. PAgP is a Cisco-proprietary protocol that can be run only on Cisco switches and those switches released by licensed vendors. LACP, which is defined in IEEE 802.3ad, allows Cisco switches to manage Ethernet channeling with devices that conform to the 802.3ad specification.

Note MAC address notification settings are ignored on PAgP and LACP EtherChannel ports.

To use PAgP, see the "Understanding the Port Aggregation Protocol" section on page 6-5. To use LACP, see the "Understanding the Link Aggregation Control Protocol" section on page 6-12.

EtherChannel Configuration Guidelines

If improperly configured, some EtherChannel ports are disabled automatically to avoid network loops and other problems. Follow these guidelines to avoid configuration problems.

Note Except where specifically differentiated, these guidelines apply to both PAgP and LACP.

These sections provide EtherChannel configuration guidelines:

- Guidelines for Port Configuration, page 6-3
- Guidelines for VLAN and Trunk Configuration, page 6-4
- EtherChannel Interaction with Other Features, page 6-4

Guidelines for Port Configuration

Follow these port configuration guidelines:

- You can have a maximum of eight compatibly configured ports per EtherChannel; the ports do not have to be contiguous or on the same module.

  Note To configure the EtherChannel across different modules, you must put the ports in the same administrative group using the **set port channel** *port_list admin_group* command.

- All ports in an EtherChannel must use the same protocol; you cannot run two protocols on one module.
- PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

  Note Switches can be configured manually with PAgP on one side and LACP on the other side in the **on** mode.

- You can change the protocol at any time, but this change causes all existing EtherChannels to reset to the default channel mode for the new protocol.
- Configure all ports in an EtherChannel to operate at the same speed and duplex mode (full duplex only for LACP mode).
- Enable all ports in an EtherChannel. If you disable a port in an EtherChannel, it is treated as a link failure and its traffic is transferred to one of the remaining ports in the EtherChannel.
- A port cannot belong to more than one channel group at the same time.
- Ports with different port path costs, set by the **set spantree portcost** command, can form an EtherChannel as long as they are otherwise compatibly configured. Setting different port path costs does not, by itself, make ports incompatible for the formation of an EtherChannel.

6058

- PAgP and LACP manage channels differently. When all the ports in a channel get disabled, PAgP removes them from its internal channels list; **show** commands do not display the channel. With LACP, when all the ports in a channel get disabled, LACP does not remove the channel; **show** commands continue to display the channel even though all its ports are down. To determine if a channel is actively sending and receiving traffic with LACP, use the **show port** command to see if the link is up or down.
- LACP does not support half-duplex links. If a port is in active/passive mode and becomes half duplex, the port is suspended (and a syslog message is generated). The port is shown as "connected" using the **show port** command and as "not connected" using the **show spantree** command. This discrepancy is because the port is physically connected but never joined spanning tree. To get the port to join spanning tree, either set the duplex to full or set the channel mode to off for that port.

  With software releases 7.3(1) and later, LACP behavior for half-duplex links has changed and affected ports are no longer suspended. Instead of suspending a port, LACP PDU transmission (if any) is suppressed. If the port is part of a channel, the port is detached from the channel but still functions as a nonchannel port. A syslog message is generated when this condition occurs. Normal LACP behavior is reenabled automatically when the link is set back to full duplex.

Guidelines for VLAN and Trunk Configuration

Follow these VLAN and trunk-related guidelines:

- Assign all ports in an EtherChannel to the same VLAN, or configure them as trunk ports.
- If you configure the EtherChannel as a trunk, configure the same trunk mode on all the ports in the EtherChannel. Configuring ports in an EtherChannel in different trunk modes can have unexpected results.
- An EtherChannel supports the same allowed range of VLANs on all the ports in a trunking EtherChannel. If the allowed range of VLANs is not the same for a port list, the ports do not form an EtherChannel even when set to the **auto** or **desirable** mode with the **set port channel** command.
- Do not configure the ports in an EtherChannel as dynamic VLAN ports. Doing so can adversely affect switch performance.
- Ports with different VLAN cost configurations cannot form a channel.

EtherChannel Interaction with Other Features

Follow these guidelines associated with EtherChannel's interaction with other features:

- An EtherChannel will not form with ports that have different GARP VLAN Registration Protocol (GVRP), GARP Multicast Registration Protocol (GMRP), and QoS configurations.
- An EtherChannel will not form with ports where the port security feature is enabled. You cannot enable the port security feature for ports in an EtherChannel.
- An EtherChannel will not form if one of the ports is a SPAN destination port.
- An EtherChannel will not form if protocol filtering is set differently on the ports.
- Cisco Discovery Protocol (CDP) runs on the physical port even after the port is added to a channel.
- VLAN Trunking Protocol (VTP) and Dual Ring Protocol (DRiP) run on the channel.
- During fast switchover to the standby supervisor engine, all channeling ports are cleared on its channeling configuration and state, and the links are pulled down temporarily to cause partner ports to reset. All ports are reset to the nonchanneling state.

- Ports with different dot1q port types cannot form a channel.
- Ports with different jumbo frame configurations cannot form a channel.
- Ports with different dynamic configurations cannot form a channel.
- During high-availability switchover to the standby supervisor engine, all channeling ports remain operational. Ports are reset only if there are events missing during the switchover.

Note With software releases 6.3(1) and later, a PAgP-configured EtherChannel is preserved even if it contains only one port (this does not apply to LACP-configured EtherChannels). In software releases prior to 6.3(1), traffic was disrupted when you removed a 1-port channel from spanning tree and then added it to spanning tree as an individual port.

Note With software releases 6.3(1) and later, due to the port ID handling by the spanning tree feature, the maximum number of EtherChannels is 126 for a 6- or 9-slot chassis and 63 for a 13-slot chassis.

Understanding the Port Aggregation Protocol

Note Use the information in these sections if you are configuring EtherChannel using PAgP. If you are using LACP, see the "Understanding the Link Aggregation Control Protocol" section on page 6-12.

These sections describe PAgP:

- PAgP Modes, page 6-5
- PAgP Administrative Groups, page 6-6
- PAgP EtherChannel IDs, page 6-7

PAgP Modes

PAgP facilitates the automatic creation of EtherChannels by exchanging packets between Ethernet ports. PAgP packets are exchanged only between ports in **auto** and **desirable** modes. Ports configured in **on** or **off** mode do not exchange PAgP packets. The protocol learns the capabilities of port groups dynamically and informs the other ports. After PAgP identifies correctly matched EtherChannel links, it groups the ports into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

EtherChannel includes four user-configurable modes: **on**, **off**, **auto**, and **desirable**. Only **auto** and **desirable** are PAgP modes. You can modify the **auto** and **desirable** modes with the **silent** and **non-silent** keywords. By default, ports are in **auto silent** mode.

6050

Table 6-1 describes the EtherChannel modes available in PAgP.

Table 6-1 EtherChannel Modes Available in PAgP

Mode	Description
on	Mode that forces the port to channel without PAgP. With the **on** mode, a usable EtherChannel exists only when a port group in **on** mode is connected to another port group in **on** mode.
off	Mode that prevents the port from channeling.
auto	PAgP mode that places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP packet negotiation. (Default)
desirable	PAgP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending PAgP packets.
silent	Keyword that is used with the **auto or desirable** mode when no traffic is expected from the other device to prevent the link from being reported to the Spanning Tree Protocol as down. (Default)
non-silent	Keyword that is used with the **auto** or **desirable** mode when traffic is expected from the other device.

Both the **auto** and **desirable** modes allow ports to negotiate with connected ports to determine if they can form an EtherChannel, based on criteria such as port speed, trunking state, and VLAN numbers.

Ports can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:

- A port in **desirable** mode can form an EtherChannel successfully with another port that is in **desirable** or **auto** mode.
- A port in **auto** mode can form an EtherChannel with another port in **desirable** mode.
- A port in **auto** mode cannot form an EtherChannel with another port that is also in **auto** mode, because neither port will initiate negotiation.

When configurable, EtherChannel frame distribution can use MAC addresses, IP addresses, and Layer 4 port numbers. You can specify either the source or the destination address or both the source and destination addresses and Layer 4 port numbers. The mode you select applies to all EtherChannels configured on the switch. Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel is going to a single MAC address only, using source addresses, IP addresses, or Layer 4 port numbers as the basis for frame distribution may provide better frame distribution than selecting MAC addresses as the basis.

PAgP Administrative Groups

Configuring an EtherChannel creates an administrative group, designated by an integer between 1 and 1024, to which the EtherChannel belongs. When an administrative group is created, you can assign an administrative group number or let the next available administrative group number be assigned automatically. Forming a channel without specifying an administrative group number creates a new automatically numbered administrative group. An administrative group may contain a maximum of eight ports.

PAgP EtherChannel IDs

Each EtherChannel is automatically assigned a unique EtherChannel ID. Use the **show channel group** *admin_group* command to display the EtherChannel ID.

Configuring EtherChannel Using PAgP

These sections describe how to configure EtherChannel using PAgP:

- Specifying the EtherChannel Protocol, page 6-7
- Configuring an EtherChannel, page 6-8
- Setting the EtherChannel Port Mode, page 6-8
- Setting the EtherChannel Port Path Cost, page 6-8
- Setting the EtherChannel VLAN Cost, page 6-9
- Configuring EtherChannel Load Balancing, page 6-11
- Displaying EtherChannel Traffic Utilization, page 6-11
- Displaying Outgoing Ports for a Specified Address or Layer 4 Port Number, page 6-12
- Disabling an EtherChannel, page 6-12

Note Before you configure the EtherChannel, see the "EtherChannel Configuration Guidelines" section on page 6-3.

Specifying the EtherChannel Protocol

Note The default protocol is PAgP.

Note You can specify only one protocol, PAgP or LACP, per module.

To specify the EtherChannel protocol, perform this task in privileged mode:

Task	Command
Specify the EtherChannel protocol.	**set channelprotocol [pagp | lacp]** *mod*

This example shows how to specify the PAgP protocol for module 3:

```
Console> (enable) set channelprotocol pagp 3
Channeling protocol set to PAGP for module(s) 3.
Console> (enable)
```

6059

Configuring an EtherChannel

To configure EtherChannel on a group of Ethernet ports, perform this task in privileged mode:

Task	Command
Configure the EtherChannel on the desired ports.	**set port channel** *mod/ports...* [*admin_group*] **set port channel** *mod/ports...* **mode** {**on** | **off** | **desirable** | **auto**} [**silent** | **non-silent**]

This example shows how to configure a seven-port EtherChannel in a new administrative group:

```
Console> (enable) set port channel 2/2-8 mode desirable
Ports 2/2-8 left admin_group 1.
Ports 2/2-8 joined admin_group 2.
Console> (enable)
```

Setting the EtherChannel Port Mode

To set a port's EtherChannel mode, perform this task in privileged mode:

Task	Command
Set a port's EtherChannel mode.	**set port channel** *mod/ports...* [*admin_group*] **set port channel** *mod/port* **mode** {**on** | **off** | **desirable** | **auto**} [**silent** | **non-silent**]

This example shows how to set port 2/1 to **auto** mode:

```
Console> (enable) set port channel 2/1 mode auto
Ports 2/1 channel mode set to auto.
Console> (enable)
```

Setting the EtherChannel Port Path Cost

Note You accomplish this task using a global command that configures both LACP and PAgP.

The channel path cost is achieved by adjusting the port costs of each port belonging to the channel. If you do not specify the cost, it is updated based on the current port costs of the channeling ports. You may address one channel or all channels.

To set the EtherChannel port path cost, perform this task in privileged mode:

	Task	Command
Step 1	Use the administrative group number to display the EtherChannel ID.	**show channel group** *admin_group* or **show lacp-channel group** *admin_key*
Step 2	Use the EtherChannel ID to set the EtherChannel port path cost.	**set spantree channelcost** {*channel_id* | **all**} *cost*

Note When you enter the **set spantree channelcost** command, it does not appear in the configuration file. The command causes a "set spantree portcost" entry to be created for each port in the channel. See the "Configuring the PVST+ Port Cost" section in Chapter 8, "Configuring Spanning Tree," for information on using the **set spantree portcost** command.

This example shows how to set the EtherChannel port path cost for channel ID 768:

```
Console> (enable) show channel group 20
Admin Port  Status     Channel   Channel
group                  Mode      id
----- ----- ---------- --------- --------
  20    1/1 notconnect on             768
  20    1/2 connected  on             768

Admin Port  Device-ID                       Port-ID                   Platform
group
----- ----- ------------------------------- ------------------------- ----------
  20    1/1
  20    1/2  066510644(cat26-lnf(NET25))     2/1                       WS-C6009
Console> (enable)

Console> (enable) set spantree channelcost 768 12
Port(s) 1/1,1/2 port path cost are updated to 31.
Channel 768 cost is set to 12.
Warning:channel cost may not be applicable if channel is broken.
Console> (enable)
```

Setting the EtherChannel VLAN Cost

Note You accomplish this task using a global command that configures both LACP and PAgP.

The EtherChannel VLAN cost feature provides load balancing of VLAN traffic across multiple channels configured with trunking.

You enter the **set spantree channelvlancost** command to set the initial spanning tree costs for all VLANs in the channel. The **set spantree channelvlancost** command provides an alternate cost for some of the VLANs in the channel (assuming you are trunking across the channel). This command allows you to have up to two different spanning tree costs assigned per channel; some VLANs in the channel can have the "vlancost" while the remaining VLANs in the channel have the "cost."

The **set spantree channelvlancost** command creates a "set spantree portvlancost" entry to the configuration file for each port in the channel. Once you have entered the **set spantree channelvlancost** command, you must enter the **set spantree portvlancost** command for at least one port in the channel, specifying the VLAN or VLANs that you want associated with each port. The following examples show what occurs when each command is entered:

```
Console> (enable) set spantree channelvlancost 856 10
Port(s) 3/47-48 vlan cost are updated to 16.
Channel 856 vlancost is set to 10.
```

The following commands are added to the configuration file:

- **set spantree portvlancost 3/47 cost 16**
- **set spantree portvlancost 3/48 cost 16**

Now you have to add the desired VLANs to the above created commands by entering the following:

```
Console> (enable) set spantree portvlancost 3/47 cost 16 1-1005
Port 3/47 VLANs 1025-4094 have path cost 19.
Port 3/47 VLANs 1-1005 have path cost 16.
Port 3/48 VLANs 1-1005 have path cost 16.
```

To set the EtherChannel VLAN cost, perform this task in privileged mode:

	Task	Command
Step 1	Use the administrative group number to display the EtherChannel ID.	**show channel group** *admin_group* or **show lacp-channel group** *admin_key*
Step 2	Use the EtherChannel ID to set the EtherChannel VLAN cost.	**set spantree channelvlancost** *channel_id cost*
Step 3	Configure the port cost for the desired VLANs on each port.	**set spantree portvlancost** {*mod/port*} [**cost** *cost*] [*vlan_list*]

This example shows how to set the EtherChannel VLAN cost for channel ID 856:

```
Console> (enable) show channel group 22
Admin Port  Status     Channel   Channel
group                  Mode      id
----- ----- ---------- --------- --------
   22   1/1 notconnect on             856
   22   1/2 connected  on             856

Admin Port  Device-ID                       Port-ID                   Platform
group
----- ----- ------------------------------- ------------------------- ----------
   22   1/1
   22   1/2  066510644(cat26-lnf(NET25))     2/1                       WS-C6009
Console> (enable)

Console> (enable) set spantree channelvlancost 856 10
Port(s) 3/47-48 vlan cost are updated to 16.
Channel 856 vlancost is set to 10.
Console> (enable) set spantree portvlancost 3/47 cost 16 1-1005
Port 3/47 VLANs 1025-4094 have path cost 19.
Port 3/47 VLANs 1-1005 have path cost 16.
Port 3/48 VLANs 1-1005 have path cost 16.
Console> (enable)
```

Configuring EtherChannel Load Balancing

The load-balancing policy (frame distribution) can be based on a MAC address (Layer 2), an IP address (Layer 3), or a port number (Layer 4). These policies can be activated, respectively, by the **mac**, **ip** and **session** keywords. The load balancing can be based solely on the source address (**source** keyword), destination address (**destination** keyword), or both source and destination addresses (**both** keyword).

If a packet does not belong to a selected category, the next lower level category is considered. If the hardware cannot support the frame distribution method selected, a "Feature not supported" error message is displayed.

To configure EtherChannel load balancing, perform this task in privileged mode:

Task	Command
Configure EtherChannel load balancing.	**set port channel all distribution** {**ip** | **mac** | **session**} [**source** | **destination** | **both**]

Note The **set port channel all distribution session** command option is supported on Supervisor Engine 2 only.

This example shows how to configure EtherChannel to use MAC source addresses:

```
Console> (enable) set port channel all distribution mac source
Channel distribution is set to mac source.
Console> (enable)
```

Displaying EtherChannel Traffic Utilization

To display the traffic utilization on the EtherChannel ports, perform this task:

Task	Command
Display traffic utilization.	**show channel traffic**

This example shows how to display traffic utilization on EtherChannel ports:

```
Console> (enable) show channel traffic
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   808  2/16   0.00%   0.00%  50.00%  75.75%   0.00%   0.00%
   808  2/17   0.00%   0.00%  50.00%  25.25%   0.00%   0.00%
   816  2/31   0.00%   0.00%  25.25%  50.50%   0.00%   0.00%
   816  2/32   0.00%   0.00%  75.75%  50.50%   0.00%   0.00%
Console> (enable)
```

6050

Displaying Outgoing Ports for a Specified Address or Layer 4 Port Number

To display the outgoing port used in an EtherChannel for a specific address or Layer 4 port number, perform this task:

<table>
<tr><th>Task</th><th>Command</th></tr>
<tr><td>Display the outgoing port for a specified address or Layer 4 port number.</td><td><b>show channel hash</b> <i>channel_id src_ip_addr</i> [<i>dest_ip_addr</i>] | <i>dest_ip_address</i> | <i>src_mac_addr</i> [<i>dest_mac_addr</i>] | <i>dest_mac_addr</i> | <i>src_port dest_port</i> | <i>dest_port</i></td></tr>
</table>

This example shows how to display the outgoing port for the specified source and destination IP addresses:

```
Console> (enable) show channel hash 808 172.20.32.10 172.20.32.66
Selected channel port:2/17
Console> (enable)
```

Disabling an EtherChannel

To disable an EtherChannel, perform this task in privileged mode:

Task	Command
Disable an EtherChannel.	**set port channel** *mod/port* **mode off**

This example shows how to disable an EtherChannel:

```
Console> (enable) set port channel 2/2-8 mode off
Ports 2/2-8 channel mode set to off.
Console> (enable)
```

Understanding the Link Aggregation Control Protocol

Note Use the information in these sections if you are configuring EtherChannel using LACP. If you are using PAgP, see the "Understanding the Port Aggregation Protocol" section on page 6-5.

This section contains the following descriptions:

- LACP Modes, page 6-13
- LACP Parameters, page 6-13

LACP Modes

You may manually turn on channeling by setting the port channel mode to **on**, and you may turn off channeling by setting the port channel mode to **off**.

If you want LACP to handle channeling, use the **active** and **passive** channel modes. To start automatic EtherChannel configuration with LACP, you need to configure at least one end of the link to **active** mode to initiate channeling, because ports in **passive** mode passively respond to initiation and never initiate the sending of LACP packets.

Table 6-2 describes the EtherChannel modes available in LACP.

Table 6-2 EtherChannel Modes Available in LACP

Mode	Description
on	Mode that forces the port to channel without LACP. With the **on** mode, a usable EtherChannel exists only when a port group in **on** mode is connected to another port group in **on** mode.
off	Mode that prevents the port from channeling.
passive	LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP packet negotiation. (Default)
active	LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.

LACP Parameters

The parameters used in configuring LACP are as follows:

- System priority

  Each switch running LACP must be assigned a system priority that can be specified automatically or through the CLI (see the "Specifying the System Priority" section on page 6-15). The system priority is used with the switch MAC address to form the system ID and is also used during negotiation with other systems.

- Port priority

  Each port in the switch must be assigned a port priority that can be specified automatically or through the CLI (see the "Specifying the Port Priority" section on page 6-15). The port priority is used with the port number to form the port identifier. The port priority is used to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

- Administrative key

  Each port in the switch must be assigned an administrative key value that can be specified automatically or through the CLI (see the "Specifying an Administrative Key Value" section on page 6-16). The ability of a port to aggregate with other ports is defined with the administrative key. A port's ability to aggregate with other ports is determined by these factors:

  - Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium
  - Configuration constraints that you establish

When enabled, LACP always tries to configure the maximum number of compatible ports in a channel, up to the maximum allowed by the hardware (eight ports). If LACP is not able to aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails.

You can configure different channels with ports that have been assigned the same administrative key. For example, if eight ports are assigned the same administrative key, you may configure four ports in a channel using LACP **active** mode and the remaining four ports in a manually configured channel using the **on** mode. An administrative key is meaningful only in the context of the switch that allocates it; there is no global significance to administrative key values.

Configuring EtherChannel Using LACP

These sections describe how to configure EtherChannel using LACP:

- Specifying the EtherChannel Protocol, page 6-14
- Specifying the System Prior ty, page 6-15
- Specifying the Port Priority, page 6-15
- Specifying an Administrative Key Value, page 6-16
- Changing the Channel Mode, page 6-17
- Specifying the Channel Path Cost, page 6-17
- Specifying the Channel VLAN Cost, page 6-17
- Configuring Channel Load Balancing, page 6-17
- Clearing LACP Statistics, page 6-18
- Displaying EtherChannel Traffic Utilization, page 6-18
- Displaying Outgoing Ports for a Specified Address or Layer 4 Port Number, page 6-18
- Disabling an EtherChannel, page 6-19
- Displaying Spanning Tree-Related Information for EtherChannels, page 6-19

Note Before you configure the EtherChannel, see the "EtherChannel Configuration Guidelines" section on page 6-3.

Specifying the EtherChannel Protocol

Note The default protocol is PAgP.

Note You can specify only one protocol, PAgP or LACP, per module.

To specify the EtherChannel protocol, perform this task in privileged mode:

Task	Command
Specify the EtherChannel protocol.	**set channelprotocol [pagp | lacp]** *mod*

This example shows how to specify the LACP protocol for modules 2 and 3:

```
Console> (enable) set channelprotocol lacp 2,3
Mod 2 is set to LACP protocol.
Mod 3 is set to LACP protocol.
Console> (enable)
```

Use the **show channelprotocol** command to display the protocols for all modules.

Specifying the System Priority

Note Although this command is a global option, the command applies only to modules on which LACP is enabled; it is ignored on modules running PAgP.

The system priority value must be a number in the range of 1 through 65535, where higher numbers represent lower priority. The default priority is 32768.

To specify the system priority, perform this task in privileged mode:

Task	Command
Specify the system priority.	**set lacp-channel system-priority** *value*

This example shows how to specify the system priority as 20000:

```
Console> (enable) set lacp-channel system-priority 20000
LACP system priority is set to 20000
Console> (enable)
```

Use the **show lacp-channel sys-id** command to display the LACP system ID and system priority.

Specifying the Port Priority

The port priority value must be a number in the range of 1 through 255, where higher numbers represent lower priority. The default priority is 128.

To specify the port priority, perform this task in privileged mode:

Task	Command
Specify the port priority.	**set port lacp-channel** *mod/ports* **port-priority** *value*

This example shows how to specify the port priority as 10 for ports 1/1 to 1/4 and 2/6 to 2/8:

```
Console> (enable) set port lacp-channel 1/1-4,2/6-8 port-priority 10
Port(s) 1/1-4,2/6-8 port-priority set to 10.
Console> (enable)
```

Use the **show lacp-channel group** *admin_key* **info** command to display the port priority.

Specifying an Administrative Key Value

Note When the system or module configuration information stored in NVRAM is cleared, the administrative keys are assigned new values automatically. For modules, each group of four consecutive ports, beginning at the 1st, 5th, 9th and so on, are assigned a unique administrative key. Across the module, ports must have unique administrative keys. After NVRAM is cleared, the channel mode of the ports is set to "passive."

You can specify an administrative key value to a set of ports or the system automatically selects a value if you do not specify the parameter *admin_key*. In both cases, the admin_key value can range from 1 through 1024.

If you choose a value for the administrative key, and this value has already been used in the system, then all the ports originally associated with the previously assigned admin_key value are moved to another automatically assigned value, and the modules and ports that you specified in the command are assigned the admin_key value that you specified.

The maximum number of ports to which an administrative key can be assigned is eight.

The default mode for all ports being assigned the administrative key is passive. However, if the channel was previously assigned a particular mode (see the "Changing the Channel Mode" section on page 6-17), assigning the administrative key will not affect it,and the channel mode that you specified previously is maintained.

To specify the administrative key value, perform this task in privileged mode:

Task	Command
Specify the administrative key value.	**set port lacp-channel** *mod/ports* [*admin_key*]

This example shows how to assign ports 4/1 to 4/4 the same administrative key, with the system picking its value automatically:

```
Console> (enable) set port lacp-channel 4/1-4
Port(s) 4/1-4 are assigned to admin key 96.
Console> (enable)
```

This example shows how to assign ports 4/4 to 4/6 the administrative key 96 (you specify the 96). In this example, the administrative key was previously assigned to another group of ports by the system (see the previous example):

```
Console> (enable) set port lacp-channel 4/4-6 96
Port(s) 4/1-3 are moved to admin key 97.
Port(s) 4/4-6 are assigned to admin key 96.
Console> (enable)
```

This example shows the system response when more than eight ports are assigned the same administrative key value (the request is denied, and no ports are assigned administrative key 123):

```
Console> (enable) set port lacp-port channel 2/1-2,4/1-8 123
No more than 8 ports can be assigned to an admin key.
Console> (enable)
```

Use the **show lacp-channel group** command to display administrative key values for ports.

Changing the Channel Mode

You can change the channel mode for a set of ports that were previously assigned the same administrative key (see the "Specifying an Administrative Key Value" section on page 6-16).

To change the channel mode, perform this task in privileged mode:

Task	Command
Change the channel mode.	**set port lacp-channel** *mod/ports* **mode [on | off | active | passive]**

This example shows how to change the channel mode for ports 4/1 and 4/6, setting it to **on**. The administrative key for ports 4/1 and 4/6 is unchanged.

```
Console> (enable) set port lacp-channel 4/1,4/6 mode on
Port(s) 4/1,4/6 channel mode set to on.
Console> (enable)
```

Use the **show lacp-channel group** *admin_key* command to display the channel mode for ports.

Specifying the Channel Path Cost

You can accomplish this task using a global command that configures both LACP and PAgP. For more information, see the "Setting the EtherChannel Port Path Cost" section on page 6-8.

Specifying the Channel VLAN Cost

You can accomplish this task using a global command that configures both LACP and PAgP. For more information, see the "Setting the EtherChannel VLAN Cost" section on page 6-9.

Configuring Channel Load Balancing

You can accomplish this task using a global command that configures both LACP and PAgP. For more information, see the "Configuring EtherChannel Load Balancing" section on page 6-11.

Clearing LACP Statistics

To clear LACP statistics, perform this task in privileged mode:

Task	Command
Clear LACP statistics.	**clear lacp-channel statistics**

This example shows how to clear LACP statistics:

```
Console> (enable) clear lacp-channel statistics
LACP channel counters are cleared.
Console> (enable)
```

Displaying EtherChannel Traffic Utilization

To display the traffic utilization on the EtherChannel ports, perform this task:

Task	Command
Display traffic utilization.	**show lacp-channel traffic**

This example shows how to display traffic utilization on EtherChannel ports:

```
Console> (enable) show lacp-channel traffic
ChanId Port  Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ ----- ------- ------- ------- ------- ------- -------
   808  2/16   0.00%   0.00%  50.00%  75.75%   0.00%   0.00%
   808  2/17   0.00%   0.00%  50.00%  25.25%   0.00%   0.00%
   816  2/31   0.00%   0.00%  25.25%  50.50%   0.00%   0.00%
   816  2/32   0.00%   0.00%  75.75%  50.50%   0.00%   0.00%
Console> (enable)
```

Displaying Outgoing Ports for a Specified Address or Layer 4 Port Number

To display the outgoing port used in an EtherChannel for a specific address or Layer 4 port number, perform this task:

Task	Command
Display the outgoing port for a specified address or Layer 4 port number.	**show lacp-channel hash** *channel_id src_ip_addr* [*dest_ip_addr*] | *dest_ip_address* | *src_mac_addr* [*dest_mac_addr*] | *dest_mac_addr* | *src_port dest_port* / *dest_port*

This example shows how to display the outgoing port for the specified source and destination IP addresses:

```
Console> (enable) show lacp-channel hash 808 172.20.32.10 172.20.32.66
Selected channel port:2/17
Console> (enable)
```

Disabling an EtherChannel

To disable an EtherChannel, perform this task in privileged mode:

Task	Command
Disable an EtherChannel.	**set port lacp-channel** *mod/port* **mode off**

This example shows how to disable an EtherChannel:

```
Console> (enable) set port lacp-channel 2/2-8 mode off
Port(s) 2/2-8 channel mode set to off.
Console> (enable)
```

Displaying Spanning Tree-Related Information for EtherChannels

You can display the channel ID and the truncated port list for all ports that are channeling. Ports that are not channeling are identified by their port number.

To display spanning tree-related information for EtherChannels, perform this task:

Task	Command
Display spanning-tree related information for EtherChannels.	**show spantree** *mod/port*

These examples show how to display spanning tree-related information for EtherChannels:

```
Console> show spantree 4/6
Port                     Vlan Port-State    Cost  Priority Portfast   Channel_id
------------------------ ---- ------------- ----- -------- ---------- ----------
 4/6                     1    not-connected     4       32 disabled   0
Console>

Console> show spantree 4/7
Port                     Vlan Port-State    Cost  Priority Portfast   Channel_id
------------------------ ---- ------------- ----- -------- ---------- ----------
4/7-8                    1    blocking          3       32 disabled   770
Console>
```

Apêndice ES

CHAPTER 4

Configuring Content Switching

This chapter describes how to configure content switching and contains these sections:

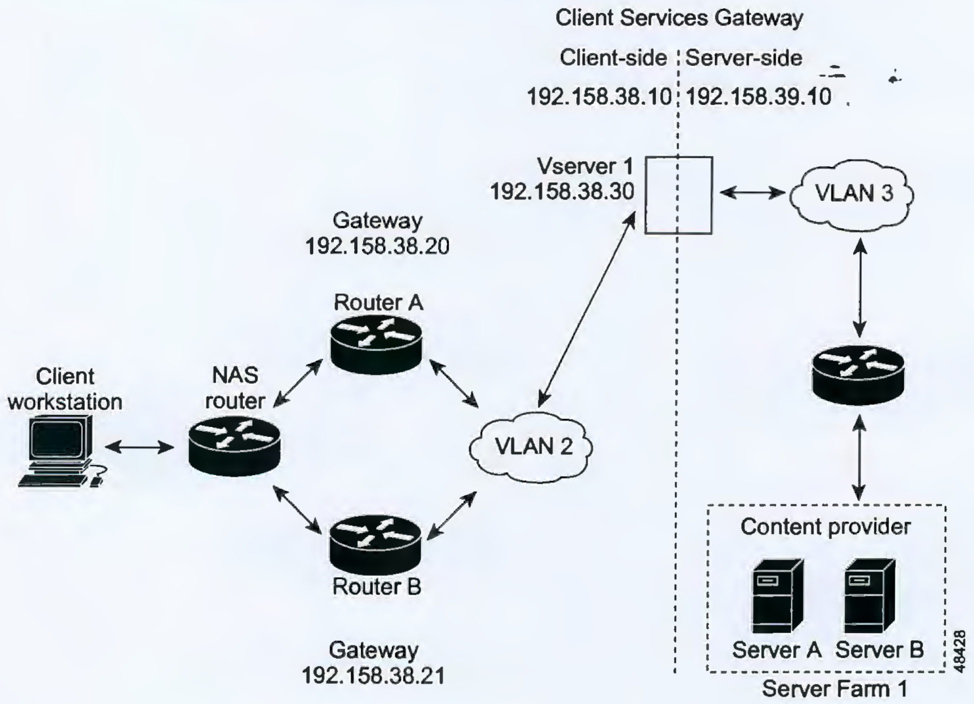
- Configuring the Single Subnet (Bridge) Mode, page 4-2
- Configuring the Secure (Router) Mode, page 4-4
- Configuring Fault Tolerance, page 4-5
- Configuring HSRP, page 4-9

Note All examples assume that the **ip slb mode csm** command has been entered as described in Chapter 3, "Configuring the Content Switching Module."

Configuring the Single Subnet (Bridge) Mode

In the single subnet (bridge) mode configuration, the client-side and server-side VLANs are on the same subnets. Figure 4-1 shows how the single subnet (bridge) mode configuration is set up.

Figure 4-1 Single Subnet (Bridge) Mode Configuration



Note	The addresses in Figure 4-1 refer to the steps in the following task table.

Note	You configure single subnet (bridge) mode by assigning the same IP address to the CSM client and server VLANs.

To configure content switching for the single subnet (bridge) mode, perform this task:

	Command	Purpose
Step 1	`Router(config-module-csm)# vlan database`	Enters the VLAN mode[1].
Step 2	`Router(vlan)# vlan 2`	Configures a client-side VLAN[2].
Step 3	`Router(vlan)# vlan 3`	Configures a server-side VLAN.
Step 4	`Router(vlan)# exit`	Exits to have the configuration take effect.
Step 5	`Router(config-module-csm)# vlan 2 client`	Creates the client-side VLAN 2 and enters the SLB VLAN mode[1].

	Command	Purpose
Step 6	`Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSM IP address on VLAN 2.
Step 7	`Router(config-slb-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway to Router A.
Step 8	`Router(config-slb-vlan-client)# gateway 192.158.38.21`	Defines the client-side VLAN gateway to Router B.
Step 9	`Router(config-slb-vserver)# vlan 3 server`	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 10	`Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSM IP address on VLAN 3.
Step 11	`Router(config-slb-vlan-client)# exit`	Exits the submode.
Step 12	`Router(config-module-csm)# vserver VIP1`	Creates a virtual server and enters the SLB *vserver* mode.
Step 13	`Router(config-slb-vserver)# virtual 192.158.38.30 tcp www`	Creates a virtual IP address.
Step 14	`Router(config-slb-vserver)# serverfarm farm1`	Associates the virtual server with the server farm[3].
Step 15	`Router(config-module-csm)# inservice`	Enables the server.

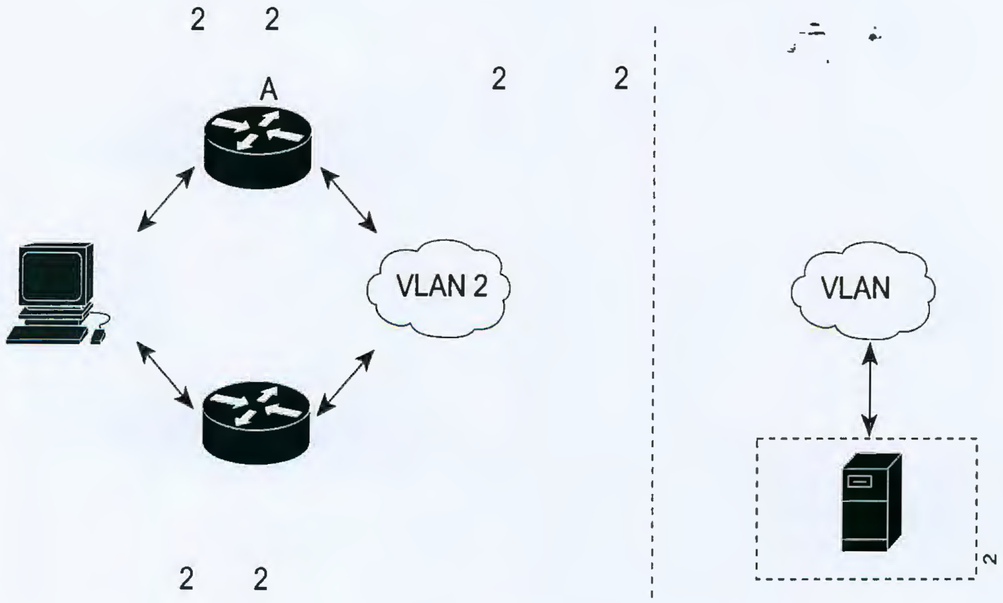
1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.
3. This step assumes that the server farm has already been configured. (See the "Configuring Server Farms" section on page 3-12.)

Note Set the server's default routes to Router A's gateway (192.158.38.20) or Router B's gateway (192.158.38.21).

Configuring the Secure (Router) Mode

In secure (router) mode, the client-side and server-side VLANs are on different subnets. Figure 4-2 shows how the secure (router) mode configuration is set up.

Figure 4-2 Secure (Router) Mode Configuration



Note The addresses in Figure 4-2 refer to the steps in the following task table.

To configure content switching in secure (router) mode, perform this task:

	Command	Purpose
Step 1	`Router(config-module-csm)# vlan database`	Enters the VLAN mode[1].
Step 2	`Router(vlan)# vlan 2`	Configures a client-side VLAN[2].
Step 3	`Router(vlan)# vlan 3`	Configures a server-side VLAN.
Step 4	`Router(vlan)# exit`	Exits to have the configuration take effect.
Step 5	`Router(config-module-csm)# vlan 2 client`	Creates the client-side VLAN 2 and enters the SLB VLAN mode.
Step 6	`Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the CSM IP address on VLAN 2.
Step 7	`Router(config-slb-vlan-client)# gateway 192.158.38.20`	Defines the client-side VLAN gateway to Router A.
Step 8	`Router(config-slb-vlan-client)# gateway 192.158.38.21`	Defines the client-side VLAN gateway to Router B.

	Command	Purpose
Step 9	`Router(config-module-csm)# vlan 3 server`	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 10	`Router(config-slb-vlan-server)# ip addr 192.158.39.10 255.255.255.0`	Assigns the CSM IP address on VLAN 3.
Step 11	`Router(config-slb-vlan-server)# exit`	Exits the submode.
Step 12	`Router(config-module-csm)# vserver VIP1`	Creates a virtual server and enters the SLB *vserver* mode.
Step 13	`Router(config-slb-vserver)# virtual 192.158.38.30 tcp www`	Creates a virtual IP address.
Step 14	`Router(config-slb-vserver)# serverfarm farm1`	Associates the virtual server with the server farm[3].
Step 15	`Router(config-module-csm)# inservice`	Enables the server.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.
3. This step assumes that the server farm has already been configured. (See the "Configuring Server Farms" section on page 3-12.)

Note Set the server's default routes to the CSM's IP address (192.158.39.10).

Configuring Fault Tolerance

This section describes a fault-tolerant configuration. In this configuration, two separate Catalyst 6500 series chassis each contain a CSM.

Note You can also create a fault-tolerant configuration with two CSMs in a single Catalyst 6500 series chassis. You also can create a fault-tolerant configuration in either the secure (router) mode or nonsecure (bridge) mode.

In the secure (router) mode, the client-side and server-side VLANs provide the fault-tolerant (redundant) connection paths between the CSM and the routers on the client side and the servers on the server side. In a redundant configuration, two CSMs perform active and standby roles. Each CSM contains the same IP, virtual server, server pool, and real server information. From the client-side and server-side networks, each CSM is configured identically. The network sees the fault-tolerant configuration as a single CSM.

Note When you configure multiple fault-tolerant CSM pairs, do not configure multiple CSM pairs to use the same FT VLAN. Use a different FT VLAN for each fault-tolerant CSM pair.

Configuring fault tolerance requires the following:

- Two CSMs that are installed in the Catalyst 6500 series chassis.
- Identically configured CSMs. One CSM is configured as the active; the other is configured as the standby.
- Each CSM connected to the same client-side and server-side VLANs.

- Communication between the CSMs provided by a shared private VLAN.
- A network that sees the redundant CSMs as a single entity.
- Connection redundancy by configuring a link that has a 1-GB per-second capacity. Enable the calendar in the switch Cisco IOS software so that the CSM state change gets stamped with the correct time.

  The following command enables the calendar:

  ```
  Cat6k-2# conf t
  Cat6k-2(config)# clock timezone WORD offset from UTC
  Cat6k-2(config)# clock calendar-valid
  ```

Because each CSM has a different IP address on the client-side and server-side VLAN, the CSM can issue health monitor probes (see the "Configuring Probes for Health Monitoring" section on page 6-1) to the network and receive responses. Both the active and standby CSMs send probes while operational. If the passive CSM assumes control, it knows the status of the servers because of the probe responses it has received.

Connection replication supports both non-TCP connections and TCP connections. Enter the **replicate csrp** {**sticky** | **connection**} command in the virtual server mode to configure replication for the CSMs.

Note The default setting for the **replicate** command is disabled.

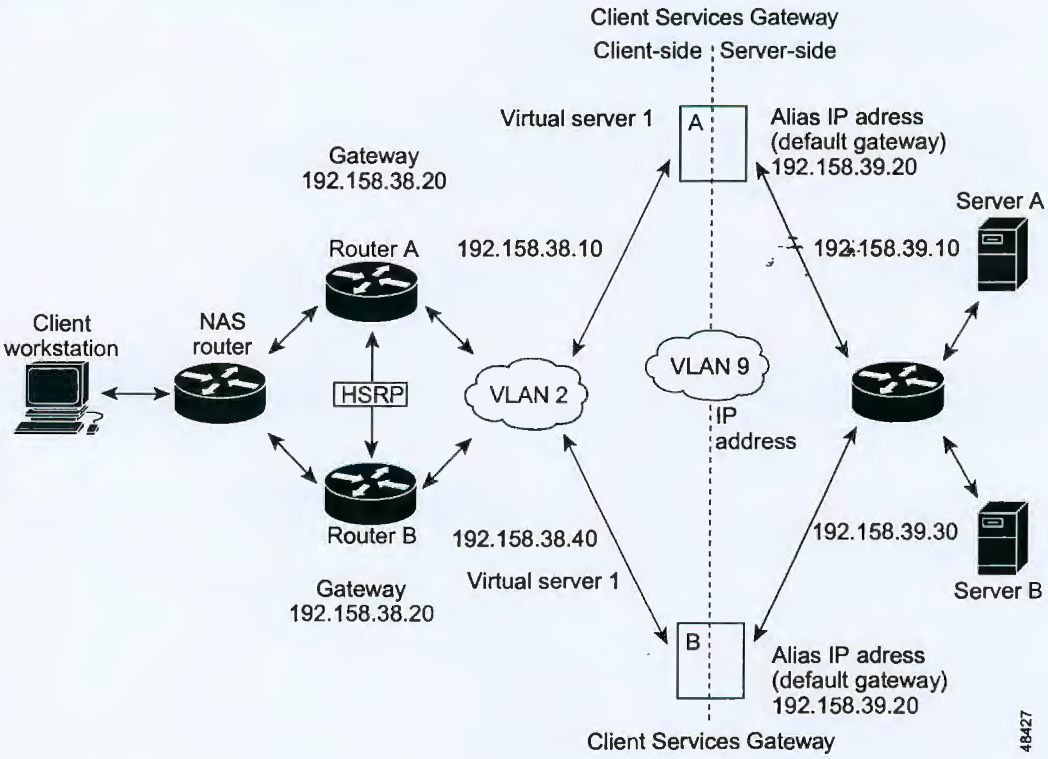
To use connection replication for connection redundancy, use these commands:

```
Cat6k-2# conf t
Cat6k-2(config)# no ip igmp snooping
```

If no router is present on the server-side VLAN, then each server's default route points to the aliased IP address.

Figure 4-3 shows how the secure (router) mode fault-tolerant configuration is set up.

Figure 4-3 Fault-Tolerant Configuration



Note The addresses in Figure 4-3 refer to the steps in the following two task tables.

To configure the active (A) CSM for fault tolerance, perform this task:

	Command	Purpose
Step 1	`Router(config-module-csm)# vlan 2 client`	Creates the client-side VLAN 2 and enters the SLB VLAN mode[1].
Step 2	`Router(config-slb-vlan-client)# ip addr 192.158.38.10 255.255.255.0`	Assigns the content switching IP address on VLAN 2.
Step 3	`Router(config-slb-vlan-client)# gateway 192.158.38.20`	(Optional) Defines the client-side VLAN gateway for an HSRP enabled gateway.
Step 4	`Router(config-module-csm)# vserver vip1`	Creates a virtual server and enters the SLB vserver mode.

	Command	Purpose
Step 5	Router(config-slb-vserver)# **virtual 192.158.38.30 tcp www**	Creates a virtual IP address.
Step 6	Router(config-module-csm)# **inservice**	Enables the server.
Step 7	Router(config-module-csm)# **vlan 3 server**	Creates the server-side VLAN 3 and enters the SLB VLAN mode.
Step 8	Router(config-slb-vlan-server)# **ip addr 192.158.39.10 255.255.255.0**	Assigns the CSM IP address on VLAN 3.
Step 9	Router(config-slb-vlan-server)# **alias ip addr 192.158.39.20 255.255.255.0**	Assigns the default route for VLAN 3.
Step 10	Router(config-slb-vlan-server) **vlan 9 ft**	Defines VLAN 9 as a fault-tolerant VLAN.
Step 11	Router(config-module-csm)# **ft group** *ft-group-number* **vlan 9**	Creates the content switching active and standby (A/B) group VLAN 9.
Step 12	Router(config-module-csm)# **vlan database**	Enters the VLAN mode[1].
Step 13	Router(vlan)# **vlan 2**	Configures a client-side VLAN 2[2].
Step 14	Router(vlan)# **vlan 3**	Configures a server-side VLAN 3.
Step 15	Router(vlan)# **vlan 9**	Configures a fault-tolerant VLAN 9.
Step 16	Router(vlan)# **exit**	Enters the **exit** command to have the configuration take affect.

[1] Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.

[2] The **no** form of this command restores the defaults.

To configure the standby (B) CSM for fault tolerance, perform this task (see Figure 4-3):

	Command	Purpose
Step 1	Router(config-module-csm)# **vlan 2 client**	Creates the client-side VLAN 2 and enters the SLB VLAN mode[1].
Step 2	Router(config-slb-vlan-client)# **ip addr 192.158.38.40 255.255.255.0**	Assigns the Content Switching IP address on VLAN 2.
Step 3	Router(config-module-csm) **vlan 9 ft**	Defines VLAN 9 as a fault-tolerant VLAN.
Step 4	Router(config-slb-vlan-client)# **gateway 192.158.38.20**	Defines the client-side VLAN gateway.
Step 5	Router(config-module-csm)# **vserver vip1**	Creates a virtual server and enters the SLB *vserver* mode.
Step 6	Router(config-slb-vserver)# **virtual 192.158.38.30 tcp www**	Creates a virtual IP address.
Step 7	Router(config-module-csm)# **inservice**	Enables the server.
Step 8	Router(config-module-csm)# **vlan 3 server**	Creates the server-side VLAN 3 and enters the SLB *vlan* mode.
Step 9	Router(config-slb-vserver)# **ip addr 192.158.39.30 255.255.255.0**	Assigns the CSM IP address on VLAN 3.
Step 10	Router(config-slb-vserver)# **alias 192.158.39.20 255.255.255.0**	Assigns the default route for VLAN 2.

	Command	Purpose

Step 11	`Router(config-module-csm)# ft group`
	`ft-group-number vlan 9`
		Creates the CSM active and standby (A/B) group VLAN 9.

Step 12	`Router(config-module-csm)# show module csm`
	`module ft`
		Displays the state of the fault tolerant system.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.

Configuring HSRP

This section provides an overview of a Hot Standby Router Protocol (HSRP) configuration (see Figure 4-4) and describes how to configure the CSMs with HSRP and CSM failover on the Catalyst 6500 series switches.

HSRP Configuration Overview

Figure 4-4 shows that two Catalyst 6500 series switches, Switch 1 and Switch 2, are configured to route from a client-side network (10.100/16) to an internal CSM client network (10.6/16, VLAN 136) through an HSRP gateway (10.100.0.1). The configuration shows the following:

- The client-side network is assigned an HSRP group ID of HSRP ID 2.
- The internal CSM client network is assigned an HSRP group ID of HSRP ID 1.

Note HSRP group 1 must have tracking turned on so that it can track the client network ports on HSRP group 2. When HSRP group 1 detects any changes in the active state of those ports, it duplicates those changes so that both the HSRP active (Switch 1) and HSRP standby (Switch 2) switches share the same knowledge of the network.

In the example configuration, two CSMs (one in Switch 1 and one in Switch 2) are configured to forward traffic between a client-side and a server-side VLAN:

- Client VLAN 136

  Note The client VLAN is actually an internal CSM VLAN network; the actual client network is on the other side of the switch.

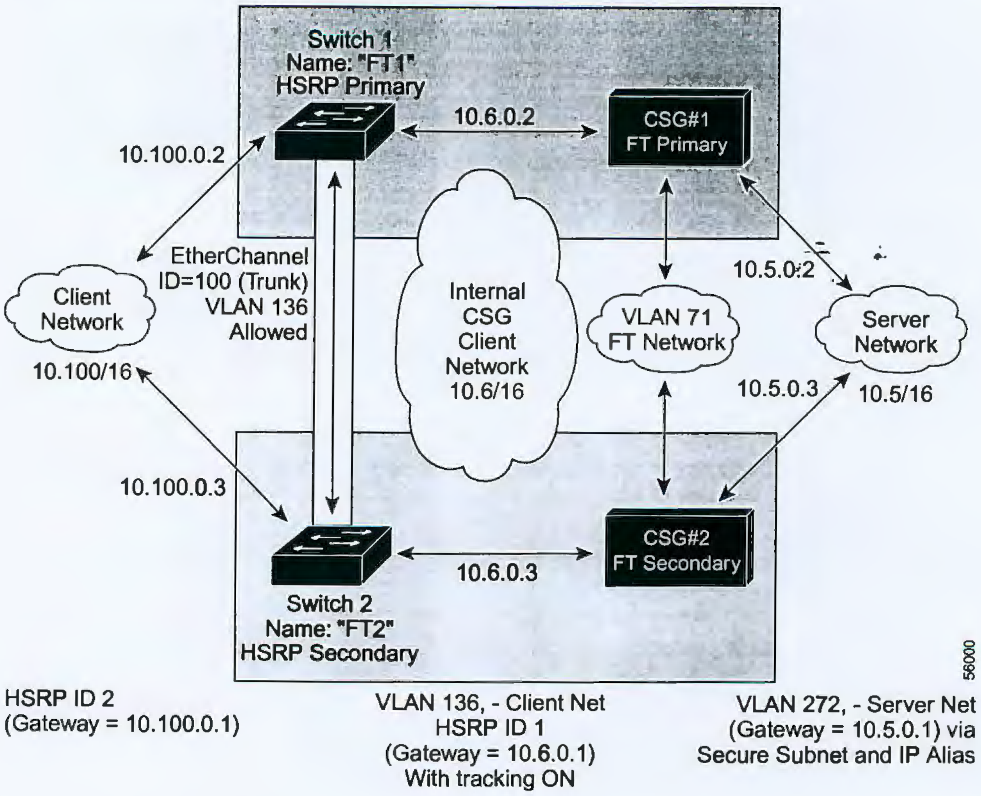
- Server VLAN 272

  The actual servers on the server network (10.5/1) point to the CSM server network through an aliased gateway (10.5.0.1), allowing the servers to run a secure subnet.

  In the example configuration, an EtherChannel is set up with trunking enabled, allowing traffic on the internal CSM client network to travel between the two Catalyst 6500 series switches. The setup is shown in Figure 4-4.

  Note EtherChannel protects against a severed link to the active switch and a failure in a non-CSM component of the switch. EtherChannel also provides a path between an active CSM in one switch and another switch, allowing CSMs and switches to fail over independently, providing an extra level of fault tolerance.

Figure 4-4 HSRP Configuration



Creating the HSRP Gateway

This procedure describes how to create an HSRP gateway for the client-side network. The gateway is HSRP ID 2 for the client-side network.

Note In this example, HSRP is set on Fast Ethernet ports 3/6.

To create an HSRP gateway, follow these steps:

Step 1 Configure Switch 1—FT1 (HSRP active) as follows:

```
Router(config)#interface FastEthernet3/6
Router(config)#ip address 10.100.0.2 255.255.0.0
Router(config)#standby 2 priority 110 preempt
Router(config)#standby 2 ip 10.100.0.1
```

Step 2 Configure Switch 2—FT2 (HSRP standby) as follows:

```
Router(config)#interface FastEthernet3/6
Router(config)#ip address 10.100.0.3 255.255.0.0
Router(config)#standby 2 priority 100 preempt
Router(config)#standby 2 ip 10.100.0.1
```

Creating Fault-Tolerant HSRP Configurations

This section describes how to create a fault-tolerant HSRP secure-mode configuration. To create a nonsecure-mode configuration, enter the commands described with these exceptions:

- Assign the same IP address to both the server-side and the client-side VLANs.
- Do not use the **alias** command to assign a default gateway for the server-side VLAN.

To create fault-tolerant HSRP configurations, follow these steps:

Step 1 Configure VLANs on HSRP FT1 as follows:

```
Router(config)# module csm 5
Router(config-module-csm)# vlan 136 client
Router(config-slb-vlan-client)# ip address 10.6.0.245 255.255.0.0
Router(config-slb-vlan-client)# gateway 10.6.0.1
Router(config-slb-vlan-client)# exit

Router(config-module-csm)# vlan 272 server
Router(config-slb-vlan-server)# ip address 10.5.0.2 255.255.0.0
Router(config-slb-vlan-server)# alias 10.5.0.1 255.255.0.0
Router(config-slb-vlan-server)# exit

Router(config-module-csm)# vlan 71 ft

Router(config-module-csm)# ft group 88 vlan 71
Router(config-slb-ft)# priority 30
Router(config-slb-ft)# preempt
Router(config-slb-ft)# exit

Router(config-module-csm)# interface Vlan136
ip address 10.6.0.2 255.255.0.0
standby 1 priority 100 preempt
standby 1 ip 10.6.0.1
standby 1 track Fa3/6 10
```

Step 2 Configure VLANs on HSRP FT2 as follows:

```
Router(config)# module csm 6
Router(config-module-csm)# vlan 136 client
Router(config-slb-vlan-client)# ip address 10.6.0.246 255.255.0.0
Router(config-slb-vlan-client)# gateway 10.6.0.1
Router(config-slb-vlan-client)# exit

Router(config-module-csm)# vlan 272 server
Router(config-slb-vlan-server)# ip address 10.5.0.3 255.255.0.0
Router(config-slb-vlan-server)# alias 10.5.0.1 255.255.0.0
Router(config-slb-vlan-server)# exit

Router(config-module-csm)# vlan 71 ft
Router(config-module-csm)# ft group 88 vlan 71
Router(config-slb-ft)# priority 20
Router(config-slb-ft)# preempt
Router(config-slb-ft)# exit

Router(config-module-csm)# interface Vlan136
ip address 10.6.0.3 255.255.0.0
standby 1 priority 100 preempt
standby 1 ip 10.6.0.1
standby 1 track Fa3/6 10
```

Note To allow tracking to work, preempt must be on.

Step 3 Configure EtherChannel on both switches as follows:

```
Router(console)# interface Port-channel100
Router(console)# switchport
Router(console)# switchport trunk encapsulation dot1q
Router(console)# switchport trunk allowed vlan 136
```

Note By default, all VLANs are allowed on the port channel.

Step 4 To prevent problems, remove the server and FT CSM VLANs as follows:

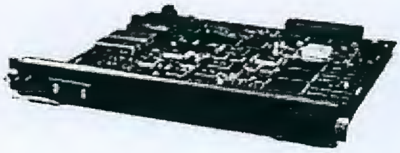
```
Router(console)# switchport trunk remove vlan 71
Router(console)# switchport trunk remove vlan 272
```

Step 5 Add ports to the EtherChannel as follows:

```
Router(console)# interface FastEthernet3/25
Router(console)# switchport
Router(console)# channel-group 100 mode on
```

Apêndice E1

Cisco **Catalyst 6500** Series Content Switching Module

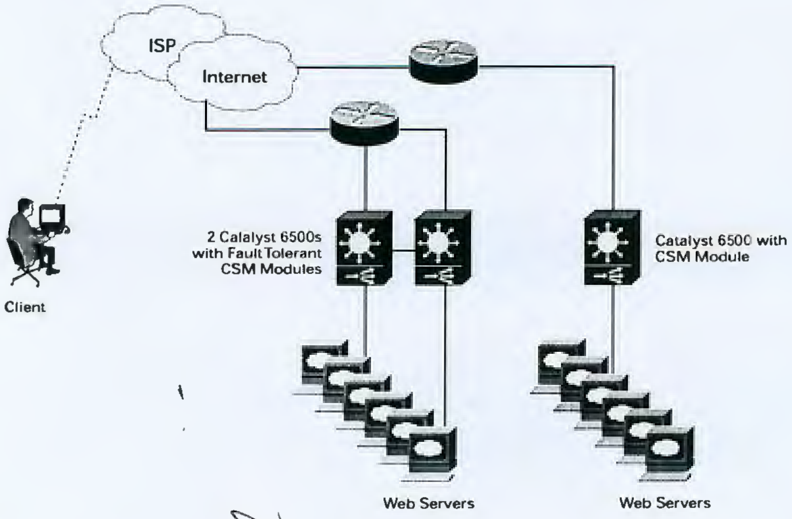


The Cisco Content Switching Module (CSM) is a Cisco Catalyst® 6500 line card that balances client traffic to farms of servers, firewalls, Secure Sockets Layer (SSL) devices, or virtual private network (VPN) termination devices. The Cisco CSM provides a high-performance, cost-effective load-balancing solution for enterprise and Internet service provider (ISP) networks. The Cisco CSM meets the demands of high-speed content delivery networks, tracking network sessions and server load conditions in real time and directing each session to the most appropriate server. Fault-tolerant Cisco CSM configurations maintain full state information and provide true hitless failover required for mission-critical functions.

The Cisco CSM provides the following key benefits (refer to Figure 1):

- Market-leading performance—The Cisco CSM establishes up to 165,000 Layer 4 connections per second (depending on software version) and provides high-speed content switching while maintaining 1 million concurrent connections.
- Outstanding price/performance value for large data centers and ISPs—The Cisco CSM features a low connection cost and occupies a small footprint. It slides into a slot in a new or existing Cisco Catalyst 6500 and enables all ports in the Cisco Catalyst 6500 for Layer 4–7 content switching.
- Multiple Cisco CSMs can be installed in the same Cisco Catalyst 6500.
- Ease of configuration—The Cisco CSM uses the same Cisco IOS® command-line interface (CLI) that is used to configure the Cisco Catalyst 6500 Switch.

Figure 1. The Cisco CSM



Content Switching Module Key Features

Firewall Load Balancing

The Cisco CSM allows you to scale firewall protection by distributing traffic across multiple firewalls on a per-connection basis, while ensuring that all packets belonging to a particular connection go through the same firewall. Both stealth and regular firewalls are supported.

URL and Cookie-Based Load Balancing

The Cisco CSM allows full regular expression pattern matching for policies based on URLs, cookies, and Hypertext Transfer Protocol (HTTP) header fields. The Cisco CSM supports any URL or cookie format—allowing it to load balance existing Web content without requiring URL/cookie format changes.

High Performance

The Cisco CSM performs up to 165,000 new Layer 4 TCP connection setups per second, depending on software version. These connections can be spread across 4096 virtual servers (16,384 real servers) and all the ports in a Cisco Catalyst 6500, or they can be focused on a single port. This provides a benefit over competitors who use distributed architectures that require use of all the ports in order to gain maximum performance.

Network Configurations

The Cisco CSM supports many different network topology types. A Cisco CSM can operate in a mixed bridged and routed configuration, allowing traffic to flow from the client side to the server side on the same or on different IP subnets.

IP Protocol Support

The Cisco CSM accommodates a wide range of common IP protocols—including TCP and User Datagram Protocol (UDP). Additionally, the Cisco CSM supports higher-level protocols, including HTTP, File Transfer Protocol (FTP), Telnet, Real-Time Streaming Protocol (RTSP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP).

User Session Stickiness

Whenever encryption or e-commerce is involved, it is important that the end user is consistently directed to the same server-that is, the server where the user's shopping cart is located or the encryption tunnel terminates. Cisco CSM User Session Stickiness provides the ability to consistently bring users back to the same server-based on SSL session ID, IP address, cookie, or HTTP redirection.

Load-Balancing Algorithms

The Cisco CSM supports the following load-balancing algorithms:

- Round robin
- Weighted Round Robin
- Least connections
- Weighted least connections
- Source and/or destination IP hash (subnet mask also configurable)
- URL hashing

Quality of Service

Providing differentiated levels of service to end users is important when generating revenue from content. The Cisco CSM takes advantage of the robust quality of service (QoS) of the Cisco Catalyst 6500, enabling traffic differentiation as follows:

- Correctly prioritizes packets based on Layer 7 rules
- Directs users who are paying more for services to faster or less loaded servers

High Availability

The Cisco CSM continually monitors server and appliation availability using health monitoring probes, inband health monitoring, return code checking, and the Dynamic Feedback Protocol (DFP). When a real server or gateway failure occurs, the Cisco CSM redirects traffic to a different location. Servers can be added and removed without disrupting service—systems can easily be scaled up or down.

Connection Redundancy

Optionally, two Cisco CSMs can be configured in a fault-tolerant configuration to share state information about user sessions and provide connection redundancy. If the active Cisco CSM fails, open connections are handled by the standby CSM without interruption, and users experience hitless failover—an important requirement for e-commerce sites and sites where encryption is used.

Global Server Load Balancing

The CSM offers multiple options for building a global or geographical load balanced environment. The CSM can act as an authoritative DNS and perform GSLB among geographically dispersed CSMs for the purposes of disaster recovery or for small GSLB environments with 2-4 locations. In addition, the CSM can report load information for it's Virtual IPs into the Global Site Selector (GSS), an appliance designed for advanced GSLB scaling up to 128 sites. With the many different GSLB options the CSM offers the ability to scale GSLB capabilities as growth demands.

Configuration Limits

- Total virtual LANs (VLANs) (client and server): 256
- Virtual servers: 4000
- Server farms: 4000

- Real servers: 16,000
- Probes: 4000
- Access control list (ACL) items: 16,000

Performance Summary
Connections
1,000,000 concurrent TCP connections
165,000 connection setups per second—Layer 4
Throughput
Total combined throughput of 4 Gigabits per second (client to server and server to client)
Cisco Catalyst Switch Platform Requirements
Cisco IOS Software only—Cisco Catalyst Operating System is not supported
Not fabric enabled—Functions as a bus-enabled line card
Multilayer Switch Feature Card (MSFC) or MSFC2
Physical Specifications
Occupies slot in the Cisco Catalyst 6500 chassis
Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm)
Weight: 5 lb (2.27 kg)
Operating Environment
Operating temperature: 32 to 104.5°F (0 to 40°C)
Nonoperating temperature: –40 to 158°F (–40 to 70°C)
Operating relative humidity: 10 to 90% (noncondensing)
Nonoperating relative humidity: 5 to 95% (noncondensing)
Operating and nonoperating altitude: Sea level to 10,000 ft (3050m)
Agency Approvals
Emissions: FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS NZS 3548 Class A
Safety: CE Marking according to UL 1950, CSA 22.2 No. 950, EN 60950, IEC 60950, TS 001, AS/NZS 3260

Cisco Catalyst 6500 CSM Ordering Information

Product Number	Product Description
WS-X6066-SLB-APC	Cisco Catalyst 6500 Content Switching Module

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: 65 317 7777
Fax: 65 317 7799

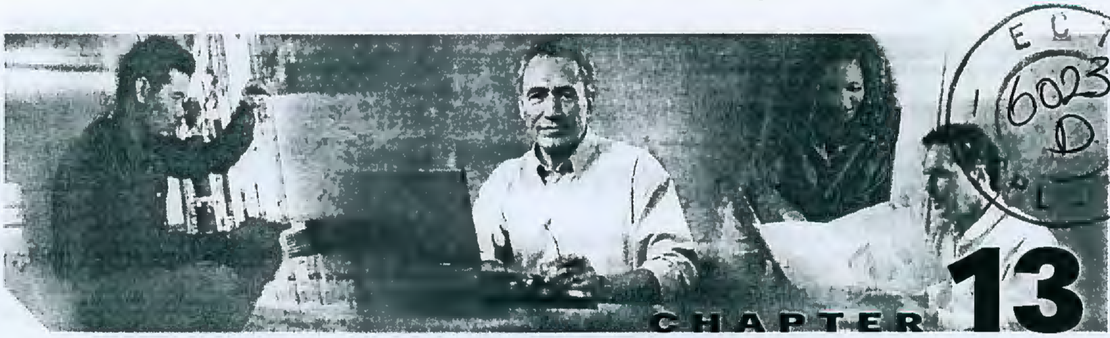
Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

Apêndice EU



CHAPTER 13

Configuring EtherChannels

This chapter describes how to configure EtherChannels on the Catalyst 6500 series switch Layer 2 or Layer 3 LAN ports.

Note

- For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.
- The commands in the following sections can be used on all LAN ports in Catalyst 6500 series switches, including the ports on the supervisor engine and a redundant supervisor engine.
- Release 12.1(13)E and later releases support the IEEE 802.3ad Link Aggregation Control Protocol (LACP).
- The WS-X6548-GE-TX and WS-X6548V-GE-TX fabric-enabled switching modules do not support more than 1 Gbps of traffic per EtherChannel, except when the switch is operating in truncated mode.
- The WS-X6148-GE-TX and WS-X6148V-GE-TX switching modules do not support more than 1 Gbps of traffic per EtherChannel.

This chapter consists of these sections:

- Understanding How EtherChannels Work, page 13-1
- EtherChannel Feature Configuration Guidelines and Restrictions, page 13-5
- Configuring EtherChannels, page 13-6

Understanding How EtherChannels Work

These sections describe how EtherChannels work:

- EtherChannel Feature Overview, page 13-1
- Understanding How EtherChannels Are Configured, page 13-2
- Understanding Port Channel Interfaces, page 13-4
- Understanding Load Balancing, page 13-5

602
D

EtherChannel Feature Overview

An EtherChannel bundles individual Ethernet links into a single logical link that provides the aggregate bandwidth of up to eight physical links.

A Catalyst 6500 series switch supports a maximum of 64 EtherChannels (256 with Release 12.1(2)E and earlier). You can form an EtherChannel with up to eight compatibly configured LAN ports on any module in a Catalyst 6500 series switch. All LAN ports in each EtherChannel must be the same speed and must all be configured as either Layer 2 or Layer 3 LAN ports.

Note The network device to which a Catalyst 6500 series switch is connected may impose its own limits on the number of ports in an EtherChannel.

If a segment within an EtherChannel fails, traffic previously carried over the failed link switches to the remaining segments within the EtherChannel. When a failure occurs, the EtherChannel feature sends a trap that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one segment in an EtherChannel are blocked from returning on any other segment of the EtherChannel.

Understanding How EtherChannels Are Configured

These sections describe how EtherChannels are configured:

- EtherChannel Configuration Overview, page 13-2
- Understanding Manual EtherChannel Configuration, page 13-3
- Understanding PAgP EtherChannel Configuration, page 13-3
- Understanding IEEE 802.3ad LACP EtherChannel Configuration, page 13-3

EtherChannel Configuration Overview

You can configure EtherChannels manually or you can use the Port Aggregation Control Protocol (PAgP) or, with Release 12.1(13)E and later, the Link Aggregation Control Protocol (LACP) to form EtherChannels. The EtherChannel protocols allow ports with similar characteristics to form an EtherChannel through dynamic negotiation with connected network devices. PAgP is a Cisco-proprietary protocol and LACP is defined in IEEE 802.3ad.

PAgP and LACP do not interoperate with each other. Ports configured to use PAgP cannot form EtherChannels with ports configured to use LACP. Ports configured to use LACP cannot form EtherChannels with ports configured to use PAgP.

Table 13-1 lists the user-configurable EtherChannel modes.

Table 13-1 EtherChannel Modes

Mode	Description
on	Mode that forces the LAN port to channel unconditionally. In the **on** mode, a usable EtherChannel exists only when a LAN port group in the **on** mode is connected to another LAN port group in the **on** mode. Because ports configured in the **on** mode do not negotiate, there is no negotiation traffic between the ports. You cannot configure the **on** mode with an EtherChannel protocol.
auto	PAgP mode that places a LAN port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP negotiation. (Default)
desirable	PAgP mode that places a LAN port into an active negotiating state, in which the port initiates negotiations with other LAN ports by sending PAgP packets.
passive	LACP mode that places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. (Default)
active	LACP mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets.

Understanding Manual EtherChannel Configuration

Manually configured EtherChannel ports do not exchange EtherChannel protocol packets. A manually configured EtherChannel forms only when you enter configure all ports in the EtherChannel compatibly.

Understanding PAgP EtherChannel Configuration

PAgP supports the automatic creation of EtherChannels by exchanging PAgP packets between LAN ports. PAgP packets are exchanged only between ports in **auto** and **desirable** modes.

The protocol learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once PAgP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

Both the **auto** and **desirable** modes allow PAgP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. Layer 2 EtherChannels also use VLAN numbers.

LAN ports can form an EtherChannel when they are in different PAgP modes if the modes are compatible. For example:

- A LAN port in **desirable** mode can form an EtherChannel successfully with another LAN port that is in **desirable** mode.
- A LAN port in **desirable** mode can form an EtherChannel with another LAN port in **auto** mode.
- A LAN port in **auto** mode cannot form an EtherChannel with another LAN port that is also in **auto** mode, because neither port will initiate negotiation.

Understanding IEEE 802.3ad LACP EtherChannel Configuration

Release 12.1(13)E and later releases support IEEE 802.3ad LACP EtherChannels. LACP supports the automatic creation of EtherChannels by exchanging LACP packets between LAN ports. LACP packets are exchanged only between ports in **passive** and **active** modes.

The protocol learns the capabilities of LAN port groups dynamically and informs the other LAN ports. Once LACP identifies correctly matched Ethernet links, it facilitates grouping the links into an EtherChannel. The EtherChannel is then added to the spanning tree as a single bridge port.

Both the **passive** and **active** modes allow LACP to negotiate between LAN ports to determine if they can form an EtherChannel, based on criteria such as port speed and trunking state. Layer 2 EtherChannels also use VLAN numbers.

LAN ports can form an EtherChannel when they are in different LACP modes as long as the modes are compatible. For example:

- A LAN port in **active** mode can form an EtherChannel successfully with another LAN port that is in **active** mode.
- A LAN port in **active** mode can form an EtherChannel with another LAN port in **passive** mode.
- A LAN port in **passive** mode cannot form an EtherChannel with another LAN port that is also in **passive** mode, because neither port will initiate negotiation.

LACP uses the following parameters:

- LACP system priority—You must configure an LACP system priority on each switch running LACP. The system priority can be configured automatically or through the CLI (see the "Configuring the LACP System Priority and System ID" section on page 13-9). LACP uses the system priority with the switch MAC address to form the system ID and also during negotiation with other systems.

  Note The LACP system ID is the combination of the LACP system priority value and the MAC address of the switch.

- LACP port priority—You must configure an LACP port priority on each port configured to use LACP. The port priority can be configured automatically or through the CLI (see the "Configuring Channel Groups" section on page 13-7). LACP uses the port priority with the port number to form the port identifier. LACP uses the port priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
- LACP administrative key—LACP automatically configures an administrative key value equal to the channel group identification number on each port configured to use LACP. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by these factors:
  - Port physical characteristics, such as data rate, duplex capability, and point-to-point or shared medium
  - Configuration restrictions that you establish

On ports configured to use LACP, LACP tries to configure the maximum number of compatible ports in an EtherChannel, up to the maximum allowed by the hardware (eight ports). If LACP cannot aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails. You can configure an additional 8 standby ports (total of 16 ports associated with the EtherChannel).

Understanding Port Channel Interfaces

Each EtherChannel has a numbered port channel interface. Release 12.1(5)E and later releases support a maximum of 64 port channel interfaces, numbered from 1 to 256.

Note Releases 12.1(4)E1, 12.1(3a)E4, and 12.1(3a)E3 support a maximum of 64 port channel interfaces, numbered from 1 to 64. Releases 12.1(2)E and earlier support a maximum of 256 port channel interfaces, numbered from 1 to 256.

The configuration that you apply to the port channel interface affects all LAN ports assigned to the port channel interface.

After you configure an EtherChannel, the configuration that you apply to the port channel interface affects the EtherChannel; the configuration that you apply to the LAN ports affects only the LAN port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply the configuration commands to the port channel interface, for example, Spanning Tree Protocol (STP) commands or commands to configure a Layer 2 EtherChannel as a trunk.

Understanding Load Balancing

An EtherChannel balances the traffic load across the links in an EtherChannel by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel.

EtherChannel load balancing can use MAC addresses or IP addresses. With a PFC2, EtherChannel load balancing can also use Layer 4 port numbers. EtherChannel load balancing can use either source or destination or both source and destination addresses or ports. The selected mode applies to all EtherChannels configured on the switch.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on an EtherChannel is going only to a single MAC address and you use the destination MAC address as the basis of EtherChannel load balancing, the EtherChannel always chooses the same link in the EtherChannel; using source addresses or IP addresses might result in better load balancing.

EtherChannel Feature Configuration Guidelines and Restrictions

When EtherChannel interfaces are configured improperly, they are disabled automatically to avoid network loops and other problems. To avoid configuration problems, observe these guidelines and restrictions:

- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannels (maximum of eight LAN ports) with no requirement that the LAN ports be physically contiguous or on the same module.
- Configure all LAN ports in an EtherChannel to use the same EtherChannel protocol; you cannot run two EtherChannel protocols in one EtherChannel.
- Configure all LAN ports in an EtherChannel to operate at the same speed and in the same duplex mode.
- LACP does not support half-duplex. Half-duplex ports in an LACP EtherChannel are put in the suspended state.

- Enable all LAN ports in an EtherChannel. If you shut down a LAN port in an EtherChannel, it is treated as a link failure and its traffic is transferred to one of the remaining ports in the EtherChannel.
- An EtherChannel will not form if one of the LAN ports is a Switched Port Analyzer (SPAN) destination port.
- For Layer 3 EtherChannels, assign Layer 3 addresses to the port channel logical interface, not to the LAN ports in the channel.
- For Layer 2 EtherChannels:
  - Assign all LAN ports in the EtherChannel to the same VLAN or configure them as trunks.
  - If you configure an EtherChannel from trunking LAN ports, verify that the trunking mode is the same on all the trunks. LAN ports in an EtherChannel with different trunk modes can operate unpredictably.
  - An EtherChannel supports the same allowed range of VLANs on all the LAN ports in a trunking Layer 2 EtherChannel. If the allowed range of VLANs is not the same, the LAN ports do not form an EtherChannel.
  - LAN ports with different STP port path costs can form an EtherChannel as long they are compatibly configured with each other. If you set different STP port path costs, the LAN ports are not incompatible for the formation of an EtherChannel.
  - An EtherChannel will not form if protocol filtering is set differently on the LAN ports.
- After you configure an EtherChannel, the configuration that you apply to the port channel interface affects the EtherChannel. The configuration that you apply to the LAN ports affects only the LAN port where you apply the configuration.
- With Release 12.1(12c)E1 and later releases, when QoS is enabled, enter the **no mls qos channel-consistency** port-channel interface command to support EtherChannels that have ports with and without strict-priority queues.

Configuring EtherChannels

These sections describe how to configure EtherChannels:

- Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels, page 13-6
- Configuring Channel Groups, page 13-7
- Configuring EtherChannel Load Balancing, page 13-10

Note

- Make sure that the LAN ports are configured correctly (see the "EtherChannel Feature Configuration Guidelines and Restrictions" section on page 13-5).
- With Release 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode commands by entering the **do** keyword before the EXEC mode command.

Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels

Note

- When configuring Layer 2 EtherChannels, you cannot put Layer 2 LAN ports into manually created port channel logical interfaces. If you are configuring a Layer 2 EtherChannel, do not perform the procedures in this section (see the "Configuring Channel Groups" section on page 13-7).
- When configuring Layer 3 EtherChannels, you must manually create the port channel logical interface as described in this section, and then put the Layer 3 LAN ports into the channel group (see the "Configuring Channel Groups" section on page 13-7).
- To move an IP address from a Layer 3 LAN port to an EtherChannel, you must delete the IP address from the Layer 3 LAN port before configuring it on the port channel logical interface.

To create a port channel interface for a Layer 3 EtherChannel, perform this task:

	Command	Purpose

Step 1	`Router(config)# interface port-channel number`
	`Router(config)# no interface port-channel number`
		Creates the port channel interface.
		Deletes the port channel interface.

Step 2	`Router(config-if)# ip address ip_address mask`	Assigns an IP address and subnet mask to the EtherChannel.
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show running-config interface port-channel number`	Verifies the configuration.

When creating the port channel interface, the *group* number can be one of the following:

- Release 12.1(5)E and later—1 through 256, up to a maximum of 64 port channel interfaces
- Releases 12.1(4)E1, 12.1(3a)E4, and 12.1(3a)E3—1 through 64
- Release 12.1(2)E and earlier—1 through 256

This example shows how to create port channel interface 1:

```
Router# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# ip address 172.32.52.10 255.255.255.0
Router(config-if)# end
```

This example shows how to verify the configuration of port channel interface 1:

```
Router# show running-config interface port-channel 1
Building configuration...

Current configuration:
!
interface Port-channel1
 ip address 172.32.52.10 255.255.255.0
 no ip directed-broadcast
end
Router#
```

Configuring Channel Groups

Note

- When configuring Layer 3 EtherChannels, you must manually create the port channel logical interface first (see the "Configuring Port Channel Logical Interfaces for Layer 3 EtherChannels" section on page 13-6), and then put the Layer 3 LAN ports into the channel group as described in this section.
- When configuring Layer 2 EtherChannels, configure the LAN ports with the **channel-group** command as described in this section, which automatically creates the port channel logical interface. You cannot put Layer 2 LAN ports into a manually created port channel interface.
- For Cisco IOS to create port channel interfaces for Layer 2 EtherChannels, the Layer 2 LAN ports must be connected and functioning.

To configure channel groups, perform this task for each LAN port:

	Command	Purpose
Step 1	`Router(config)# `**`interface`** *`type`*[1] *`slot/port`*	Selects a LAN port to configure.
Step 2	`Router(config-if)# `**`no ip address`**	Ensures that there is no IP address assigned to the LAN port.
Step 3	`Router(config-if)# `**`channel-protocol (lacp | pagp}`**	(Optional) On the selected LAN port, restricts the **channel-group** command to the EtherChannel protocol configured with the **channel-protocol** command.
	`Router(config-if)# `**`no channel-protocol`**	Removes the restriction.

Step 4	`Router(config-if)# `**`channel-group`** *`number`* **`mode`**
	`{active | auto | desirable | on | passive}`
		Configures the LAN port in a port channel and specifies the mode (see Table 13-1 on page 13-2). PAgP supports only the auto and desirable modes. LACP supports only the active and passive modes.

	`Router(config-if)# `**`no channel-group`**	Removes the LAN port from the channel group.

Step 5	`Router(config-if)# `**`lacp port-priority`**
	`priority_value`
		(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.

	`Router(config-if)# `**`no lacp port-priority`**	Reverts to the default.
Step 6	`Router(config-if)# `**`end`**	Exits configuration mode.

Step 7	`Router# `**`show running-config interface`** *`type`*[1]
	`slot/port`
	`Router# `**`show interfaces`** *`type`*[1] *`slot/port`*
	`etherchannel`
		Verifies the configuration.

[1] *type* = **ethernet, fastethernet, gigabitethernet,** or **tengigabitethernet**

This example shows how to configure Fast Ethernet ports 5/6 and 5/7 into port channel 2 with PAgP mode **desirable**:

```
Router# configure terminal
Router(config)# interface range fastethernet 5/6 -7
Router(config-if)# channel-group 2 mode desirable
Router(config-if)# end
```

Note See the "Configuring a Range of Interfaces" section on page 6-4 for information about the **range** keyword.

This example shows how to verify the configuration of port channel interface 2:

```
Router# show running-config interface port-channel 2
Building configuration...

Current configuration:
!
interface Port-channel2
 no ip address
 switchport
 switchport access vlan 10
 switchport mode access
end
Router#
```

This example shows how to verify the configuration of Fast Ethernet port 5/6:

```
Router# show running-config interface fastethernet 5/6
Building configuration...

Current configuration:
!
interface FastEthernet5/6
 no ip address
 switchport
 switchport access vlan 10
 switchport mode access
 channel-group 2 mode desirable
end
Router# show interfaces fastethernet 5/6 etherchannel
Port state     = Down Not-in-Bndl
Channel group = 12            Mode = Desirable-Sl     Gcchange = 0
Port-channel   = null         GC    = 0x00000000         Pseudo port-channel = Po1
2
Port index     = 0            Load = 0x00         Protocol =    PAgP

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.
        d - PAgP is down.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Local information:
                                Hello    Partner  PAgP     Learning  Group
Port      Flags State   Timers  Interval Count   Priority   Method  Ifindex
Fa5/2     d     U1/S1           1s       0        128        Any      0

Age of the port in the current state: 04d:18h:57m:19s
```

This example shows how to verify the configuration of port channel interface 2 after the LAN ports have been configured:

```
Router# show etherchannel 12 port-channel
                Port-channels in the group:
                ----------------------

Port-channel: Po12
------------

Age of the Port-channel   = 04d:18h:58m:50s
Logical slot/port   = 14/1          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
Protocol            =   PAgP

Router#
```

Configuring the LACP System Priority and System ID

The LACP system ID is the combination of the LACP system priority value and the MAC address of the switch.

To configure the LACP system priority and system ID, perform this task:

	Command	Purpose
Step 1	`Router(config)# lacp system-priority priority_value`	(Optional for LACP) Valid values are 1 through 65535. Higher numbers have lower priority. The default is 32768.
	`Router(config)# no lacp system-priority`	Reverts to the default.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show lacp sys-id`	Verifies the configuration.

This example shows how to configure the LACP system priority:

```
Router# configure terminal
Router(config)# lacp system-priority 23456
Router(config)# end
Router(config)#
```

This example shows how to verify the configuration:

```
Router# show lacp sys-id
23456,0050.3e8d.6400
Router#
```

The system priority is displayed first, followed by the MAC address of the switch.

Configuring EtherChannel Load Balancing

To configure EtherChannel load balancing, perform this task:

	Command	Purpose
Step 1	`Router(config)# port-channel load-balance {src-mac | dst-mac | src-dst-mac | src-ip | dst-ip | src-dst-ip | src-port | dst-port | src-dst-port}`	Configures EtherChannel load balancing.
	`Router(config)# no port-channel load-balance`	Reverts to default EtherChannel load balancing.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show etherchannel load-balance`	Verifies the configuration.

The load-balancing keywords indicate the following information:

- With a PFC2:
  - **src-port**—Source Layer 4 port
  - **dst-port**—Destination Layer 4 port
  - **src-dst-port**—Source and destination Layer 4 port
- With a PFC or PFC2:
  - **src-ip**—Source IP addresses
  - **dst-ip**—Destination IP addresses
  - **src-dst-ip**—Source and destination IP addresses
  - **src-mac**—Source MAC addresses
  - **dst-mac**—Destination MAC addresses
  - **src-dst-mac**—Source and destination MAC addresses

This example shows how to configure EtherChannel to use source and destination IP addresses:

```
Router# configure terminal
Router(config)# port-channel load-balance src-dst-ip
Router(config)# end
Router(config)#
```

This example shows how to verify the configuration:

```
Router# show etherchannel load-balance
Source XOR Destination IP address
Router#
```

Apêndice EV

APPENDIX A

Command Reference

This appendix describes the Content Switching Module (CSM) commands that are unique to server load-balancing (SLB) and Layer 3 switching.

The following commands allow you to set up and monitor SLB on the CSM:

Command	Submode Command
dfp, page A-6	agent, page A-7 manager, page A-8
ft group, page A-9	failover, page A-10 heartbeat-time, page A-11 preempt, page A-12 priority, page A-13
ip slb mode, page A-14	
map cookie, page A-16	match protocol http cookie, page A-17
map dns, page A-19	match protocol dns domain, page A-20
map header, page A-21	match protocol http header, page A-22
map retcode, page A-24	match protocol http retcode, page A-25
map url, page A-26	match protocol http url, page A-27
module csm, page A-29	
natpool, page A-30	
owner, page A-31	address, page A-32 billing-info, page A-33 contact-info, page A-34 maxconns, page A-35

Command	Submode Command
policy, page A-36	client-group, page A-37 cookie-map, page A-38 header-map, page A-39 reverse-sticky, page A-40 reverse-sticky, page A-40 set ip dscp, page A-42 sticky-group, page A-43 url-map, page A-44
probe, page A-45	address (dns), page A-47 address (icmp), page A-48 credentials, page A-49 expect status, page A-50 failed, page A-52 header, page A-53 interval, page A-54 kal-ap-udp, page A-55 name, page A-56 open, page A-58 port, page A-57 receive, page A-59 request, page A-60 retries, page A-61
probe script, page A-62	script, page A-63 failed, page A-64 interval, page A-65 open, page A-66 receive, page A-67 retries, page A-68
real, page A-69	inservice, page A-70 maxconns, page A-71 minconns, page A-72 probe, page A-73 redirect-vserver, page A-74 weight, page A-75

Command	Submode Command
redirect-vserver, page A-76	advertise, page A-77
	client, page A-78
	idle, page A-79
	inservice, page A-80
	replicate csrp, page A-81
	ssl, page A-82
	virtual, page A-83
	vlan, page A-84
	webhost backup, page A-85
	webhost relocation, page A-86
script file, page A-87	
script task, page A-88	
serverfarm, page A-89	bindid, page A-90
	failaction purge, page A-91
	health, page A-92
	nat client, page A-93
	nat server, page A-94
	predictor, page A-95
	probe, page A-97
	retcode-map, page A-98
show module csm arp, page A-99	
show module csm conns, page A-100	
show module csm dfp, page A-101	
show module csm ft, page A-103	
show module csm map, page A-104	
show module csm memory, page A-106	
show module csm natpool, page A-107	
show module csm owner, page A-108	
show module csm policy, page A-109	
show module csm probe, page A-110	
show module csm probe script, page A-112	
show module csm real, page A-113	
show module csm real retcode, page A-115	
show module csm script, page A-116	
show module csm script task, page A-117	
show module csm serverfarm, page A-118	
show module csm static, page A-120	

Command	Submode Command
show module csm static server, page A-121	
show module csm stats, page A-122	
show module csm status, page A-124	
show module csm sticky, page A-125	
show module csm tech-script, page A-126	
show module csm tech-support, page A-127	
show module csm vlan, page A-130	
show module csm vserver redirect, page A-131	
show module csm xml stats, page A-133	
snmp enable traps slb ft, page A-134	
static, page A-135	real, page A-136
vlan, page A-139	alias, page A-140 gateway, page A-141 ip address, page A-142 route, page A-143
sticky, page A-158	

Command	Submode Command
vserver, page A-144	advertise, page A-145 client, page A-146 idle, page A-147 inservice, page A-148 owner, page A-149 parse-length, page A-150 pending, page A-151 persistent rebalance, page A-152 replicate csrp, page A-153 serverfarm, page A-154 slb-policy, page A-156 ssl-sticky, page A-157 sticky, page A-158 reverse-sticky, page A-160 url-hash, page A-161 virtual, page A-162 vlan, page A-164
xml-config, page A-165	client-group, page A-166 credentials, page A-167 inservice, page A-168 port, page A-169 vlan, page A-170

dfp

Use the **dfp** command to enter the DFP submode and configure DFP. Use the **no** form of this command to remove the DFP configuration.

dfp [**password** *password* [*timeout*]]

no dfp

Syntax Description

password	(Optional) Keyword to specify a password for MD5 authentication.
password	(Optional) Password value for MD5 authentication. This password must be the same on all DFP manager devices.
timeout	(Optional) Delay period, in seconds, during which both the old password and the new password are accepted; the range is from 0 to 65535.

Defaults

The default timeout value is 180 seconds.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The timeout option allows you to change the password without stopping messages between the DFP agent and its manager.

During a timeout, the agent sends packets with the old password (or null, if there is no old password), and receives packets with either the old or new password. After a timeout expires, the agent sends and receives packets with only the new password; received packets that use the old password are discarded.

If you are changing the password for an entire load-balanced environment, set a longer timeout. The extended timeout allows enough time for you to update the password on all agents and servers before the timeout expires. It also prevents mismatches between agents and servers that have the new password and agents and servers that have the old password.

Examples

This example shows how to initiate DFP agent configuration mode, configure DFP, set the password to *flounder*, and configure a 60-second timeout:

```
SLB-Switch(config-module-csm)# dfp password flounder 60
```

Related Commands

show module csm dfp

agent

Use the **agent** command in the SLB DFP submode to configure the DFP agent to which the CSM is going to communicate. Use the **no** form of this command to remove the agent configuration.

agent *ip-address port* [*keepalive-timeout* [*retry-count* [*retry-interval*]]]

no agent *ip-address port*

Syntax Description

ip-address	IP address of the DFP agent.
port	Port number of the DFP agent.
keepalive-timeout	(Optional) Time period in seconds between keepalive messages; the range is from 1 to 65535.
retry-count	(Optional) Number of consecutive connection attempts or invalid DFP reports received before tearing down the connections and marking the agent as failed; the range is from 0 to 65535.
retry-interval	(Optional) Interval between retries; the range is from 1 to 65535.

Defaults

The *keepalive-timeout* default is 0 (no keepalive message).

Retry count default is 0 seconds (the default allows infinite retries).

The *retry-interval* default is 180 seconds.

Command Modes

SLB DFP configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to initiate the DFP agent, configure a 350-second timeout, and configure the number of retries to 270:

```
SLB-Switch(config-slb-dfp)# agent 111.101.90.10 2 350 270
```

Related Commands

dfp
manager
show module csm dfp

manager

Use the **manager** command in SLB DFP submode to set the port where an external DFP can connect to the CSM. Use the **no** form of this command to remove the manager configuration.

manager *port*

no manager

Syntax Description

port	Port number.

Defaults

This command has no default settings.

Command Modes

SLB DFP configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command enables the CSM to listen to DFP connections from an external DFP manager.

Examples

This example shows how to set the DFP manager port:

```
SLB-Switch(config-slb-dfp)# manager 4
```

Related Commands

dfp
agent
show module csm dfp

ft group

Use the **ft group** command to enter the fault-tolerant configuration submode and configure fault tolerance. Use the **no** form of this command to remove the fault-tolerant configuration.

ft group *group-id* **vlan** *vlan-id*

no ft group

Syntax Description

group-id	ID of the fault-tolerant group. Both CSMs must have the same group ID. The range is from 1 to 254.
vlan	Keyword to specify a VLAN ID.
vlan-id	ID of the VLAN over which heartbeat messages are sent. Both CSMs must have the same VLAN ID. The range is from 2 to 4095.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

A fault-tolerant group is comprised of two Catalyst 6500 series switches each containing a CSM configured for fault-tolerant operation. Each fault-tolerant group appears to network devices as a single device. A network may have more than one fault-tolerant group.

Examples

This example shows how to configure a fault-tolerant group named 123 on VLAN 5:

```
SLB-Switch(config-module-csm)# ft group 123 vlan 5
```

Related Commands

failover
heartbeat-time
preempt
priority
show module csm ft

failover

Use the **failover** command in the SLB fault-tolerant configuration submode to set the time for a standby CSM to wait before becoming an active CSM. Use the **no** form of this command to remove the failover configuration.

failover *failover-time*

no failover

Syntax Description

failover-time	Amount of time the CSM must wait after the last heartbeat message is received before assuming the other CSM is not operating; the range is from 1 to 65535.

Defaults

The default failover time is 3 seconds.

Command Modes

SLB fault-tolerant configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to set a failover period of 6 seconds:

```
SLB-Switch(config-slb-ft)# failover 6
```

Related Commands

ft group
show module csm ft

heartbeat-time

Use the **heartbeat-time** command in the SLB fault-tolerant configuration submode to set the time before heartbeat messages are transmitted by the CSM. Use the **no** form of this command to restore the default heartbeat interval.

heartbeat-time *heartbeat-time*

no heartbeat-time

Syntax Description

heartbeat-time	Time interval between heartbeat transmissions in seconds; the range is from 1 to 65535.

Defaults

The default heartbeat time is 1 second.

Command Modes

SLB fault-tolerant configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to set the heartbeat time to 2 seconds:

```
SLB-Switch(config-slb-ft)# heartbeat-time 2
```

Related Commands

ft group
show module csm ft

6000.

preempt

Use the **preempt** command in the SLB fault-tolerant configuration submode to allow a higher priority CSM to take control of a fault-tolerant group when it comes online. Use the **no** form of this command to restore the preempt default value.

preempt

no preempt

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is that preempt is not specified.

Command Modes

SLB fault-tolerant configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When you enable preempt, the higher priority CSM preempts the other CSM in the fault-tolerant group when the higher priority CSM comes online. When you enable no preempt, the current primary CSM remains the primary CSM when the next CSM comes online.

Note You must set both members of the fault-tolerant CSM pair to preempt for this feature to work.

Examples

This example shows how to set the fault-tolerance mode to preempt:

```
SLB-Switch(config-slb-ft)# preempt
```

Related Commands

ft group
priority
show module csm ft

priority

Use the priority command in the SLB fault-tolerant configuration submode to set the priority of the CSM. Use the **no** form of this command to restore the priority default value.

priority *value*

no priority

Syntax Description

value	Priority of a CSM; the range is from 1 to 254.

Defaults

The default priority value is 10.

Command Modes

SLB fault-tolerant configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The CSM with the largest priority value is the primary CSM in the fault-tolerant pair when the modules are both operating.

Examples

This example shows how to set the priority value to 12:

```
SLB-Switch(config-slb-ft)# priority 12
```

Related Commands

ft group
preempt
show module csm ft

ip slb mo e

Use the **ip slb mode** command to configure the switch to operate as a CSM load-balancing device instead of a Cisco IOS SLB load-balancing device. Use the **no** form of this command to remove the **mode** configuration.

ip slb mode {**csm** | **rp**}

no ip slb mode

No pecifying the **no ip slb mode** command is the same as specifying the **rp** mode.

Syntax Descriptim

	Keyword to select the CSM load-balancing mode that allows you to configure a single CSM only and prohibits the use of Cisco IOS SLB load-balancing on the Catalyst 6500 series switch.
	Keyword to select the route processor (Cisco IOS SLB) load-balancing mode and enable module CSM commands for configuring multiple CSMs.

Defaults

default is the **rp** mode.

Command Mo

al configuration submode.

Command Hi ase

	Modification
1)	This command was introduced.
1)	This command now enables **module csm** commands for the **rp** mode.

Usage Guide

s command allows you to change from the Cisco IOS SLB load-balancing mode to the CSM l-balancing mode.

csm mode, all **ip slb** commands apply to a CSM module; Cisco IOS SLB is not available. In **rp** mode e default), **ip slb** commands apply to Cisco IOS SLB; the **module csm** commands are available to nfigure multiple CSMs.

Examples

is example shows how to configure the switch mode:

```
B-Switch(config)# ip slb mode csm
```

Related Commands

module csm
show ip slb mode

map cookie

Use the **map cookie** command to create a cookie map and enter the cookie map configuration submode for specifying cookie match rules. Use the **no** form of this command to remove the cookie maps from the configuration.

map *cookie-map-name* **cookie**

no map *cookie-map-name*

Syntax Description

cookie-map-name	Cookie map instance; the character string is limited to 15 characters.
cookie	Keyword to enter the cookie map submode.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to create a cookie map:

```
SLB-Switch(config-module-csm)# map upnready cookie
```

Related Commands

cookie-map (SLB policy configuration submode)
match protocol http cookie
show module csm map

match protocol http cookie

Use the **match protocol http cookie** command in SLB cookie map configuration submode to add cookies to a cookie map. Multiple match rules can be added to a cookie map. Use the **no** form of this command to remove the cookie map name from the cookie map.

match protocol http cookie *cookie-name* **cookie-value** *cookie-value-expression*

Syntax Descriptionn

cookie-name	Cookie name; the range is from 1 to 63 characters.
cookie-value	Keyword to specify a cookie value expression.
cookie-value-expression	Cookie value expression string; the range is from 1 to 255 characters.

Defaults

This command has no default settings.

Command Modes

SLB cookie map configuration submode.

Usage Guidelines

Cookie regular expressions are based on the UNIX filename specification. URL expressions are stored in a cookie map in the form *cookie-name* = *cookie-value-expression*. Cookie expressions allow spaces provided they are escaped or quoted. You must match all cookies in the cookie map.

"*" means zero or more characters

"?" means exactly one character—the [Ctrl + V] key combination must be entered

"\" means escaped character

Bracketed range (for example, [0–9]) means matching any single character from the range

A leading ^ in a range means do not match any in the range

".\a" means alert (ASCII 7)

".\b" means backspace (ASCII 8

".\f" means form-feed (ASCII 12)

".\n" means newline (ASCII 10)

".\r" means carriage return (ASCII 13)

".\t" means tab (ASCII 9)

".\v" means vertical tab (ASCII 11)

".\0" means null (ASCII 0)

".\\" means backslash

".\x##" means any ASCII character as specified in two-digit hexadecimal notation

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to add cookies to a cookie map:

```
SLB-Switch(config-slb-map-cookie)# match protocol http cookie albert cookie-value 4*
```

Related Commands

cookie-map (SLB policy configuration submode)
map cookie
show module csm map

map dns

Use the **map dns** command to enter the SLB DNS map mode and configure a DNS map. Use the **no** form of this command to remove the DNS map from the configuration.

map *dns-map-name* **dns**

no map *dns-map-name*

Syntax Description

dns-map-name	Name of an SLB dns map; the character string range is from 1 to 15 characters.

Defaults

This command has no default settings.

Command Modes

SLB DNS map configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Any match of a DNS regular expression in the DNS map results in a successful match. A maximum of 1023 DNS domains can be configured to a map.

Examples

This example shows how to group DNS domains:

```
SLB-Switch(config-module-csm)# map m1 dns
SLB-Switch(config-slb-map-url)# exit
SLB-Switch(config)
```

Related Commands

match protocol dns domain
show module csm map

match protocol dns domain

Use the **match protocol dns domain** command in the SLB DNS map configuration submode to add a DNS domain to a DNS map. Use the **no** form of this command to remove the DNS domain from the URL map.

match protocol dns domain *name*

no match protocol dns domain *name*

Syntax Description

name	Names the DNS domain being mapped..

Defaults

This command has no default settings.

Command Modes

SLB DNS map configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	HTTP method parsing support was introduced.

Examples

This example shows how to adds URL expressions to a URL map:

```
SLB-Switch(config-slb-map-url)# match protocol http url Host header-value :XYZ
```

Related Commands

map dns
show module csm map

map header

Use the **map header** command to create a map group for specifying HTTP headers and enter the header map configuration submode. Use the **no** form of this command to remove the HTTP header group from the configuration.

map *name* **header**

no map *name*

Syntax Description

name	Map instance; the character string is from 1 to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to group HTTP headers and associate them with a Content Switching policy:

```
SLB-Switch(config-module-csm)# map upnready header
SLB-Switch(config-slb-map-header)# match protocol http header Accept header-value *jpeg*
SLB-Switch(config-slb-map-header)# match protocol http header User-Agent header-value *NT*
SLB-Switch(config-slb-map-header)# match protocol http header Host header-value
www.myhome.com
SLB-Switch(config-slb-map-header)# exit
```

Related Commands

header-map (SLB policy configuration submode)
match protocol http header
show module csm map

match protocol http header

Use the **match protocol http header** command in SLB header map configuration submode to specify header fields and values for the CSM to search for when receiving a request. Multiple match rules can be added to a header map. Use the **no** form of this command to remove the header match rule from the header map.

match protocol http header *field* **header-value** *expression*

no match protocol http header *field*

Syntax Description

field	Literal name of the generic field in the HTTP header. The range is from 1 to 63 characters.
header-value	Keyword to specify the header value expression.
expression	Header value regular expression string to compare against the value in the specified field; the range is from 1 to 127 characters.

Defaults

This command has no default settings.

Command Modes

SLB header map configuration submode.

Usage Guidelines

There are predefined fields, for example Accept-Language, User-Agent, or Host.

Header regular expressions are based on the UNIX filename specification. URL expressions are stored in a header map in the form *header-name* = *expression*. Header expressions allow spaces provided that they are escaped or quoted. All headers in the header map must be matched.

"*" means zero or more characters

"?" means exactly one character—the [Ctrl + V] key combination must be entered

"\" means escaped character

Bracketed range (for example, [0–9]) means matching any single character from the range

A leading ^ in a range means don't match any in the range

".\a" means alert (ASCII 7)

".\b" means backspace (ASCII 8

".\f" means form-feed (ASCII 12)

".\n" means newline (ASCII 10)

".\r" means carriage return (ASCII 13)

".\t" means tab (ASCII 9)

".\v" means vertical tab (ASCII 11)

".\0" means null (ASCII 0)

".\\" means backslash

".\x##" means any ASCII character as specified in two-digit hexadecimal notation

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to specify header fields and values to search upon a request:

```
SLB-Switch(config-slb-map-header)# match protocol http header Host header-value XYZ
```

Related Commands

header-map (SLB policy configuration submode)
map header
show module csm map

map retcode

Use the **map retcode** command to enable return error code checking and enter the return error code map submode. Use the **no** form of this command to remove the return code error checking from the configuration.

map *name* **retcode**

no map *name*

Syntax Description

name	Return error code map instance; the character string is limited to 15 characters.
retcode	Keyword to enter the return error code map submode.

Defaults

This command has no default settings.

Command Modes

Global configuration submode.

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples

This example shows how to enable return error code checking:

```
SLB-Switch(config-module-csm)# map upnready retcode
```

Related Commands

cookie-map (SLB policy configuration submode)
match protocol http cookie
show module csm map

match protocol http retcode

Use the **match protocol http retcode** command in SLB return code map configuration submode to specify return code thresholds, count and log return codes, and send syslog messages for return code events received from the servers. Use the **no** form of this command to remove the return code thresholds.

match protocol http retcode *min max* **action** {**count** | **log** | **remove**} *threshold* [**reset** *seconds*]

no match protocol http retcode *min max*

Syntax Description

min	Minimum number of return codes received before an action is taken.
max	Maximum number of return codes received before an action is taken.
action	Keyword to enable the header value expression.
count	Keyword to increment the statistics of the number of occurrences of return codes received.
log	Keyword to specify where syslog messages are sent when a threshold is reached.
remove	Keyword to specify where the syslog messages are sent when a threshold is reached and the server is removed from service.
threshold	The number of return occurrences before the log or remove action is taken.
reset	(Optional) Keyword to enable the header value expression.
seconds	Number of seconds to wait before the action can take place again.

Defaults

This command has no default settings.

Command Modes

SLB return code map configuration submode.

Usage Guidelines

The *threshold* and **reset** values are not configurable for the **count** action. These commands only are available for the **log** and **remove** actions.

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples

This example shows how to specify return codes values to search for in an HTTP request:

```
SLB-Switch(config-slb-map-retcode)# match protocol http quigly retcode 30 50 action log
400 reset 30
```

Related Commands

map retcode (SLB policy configuration submode

15986 P.

map url

Use the **map url** command to enter the SLB URL map mode and configure a URL map. Use the **no** form of this command to remove the URL map from the configuration.

map *url-map-name* **url**

no map *url-map-name*

Syntax Description

url-map-name	Name of an SLB URL map; the character string range is from 1 to 15 characters.

Defaults

This command has no default settings.

Command Modes

SLB URL map configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Any match of a URL regular expression in the URL map results in a successful match. A maximum of 1023 URLs can be configured to a map.

Examples

This example shows how to group URLs and associate them with a Content Switching policy:

```
SLB-Switch(config-module-csm)# map m1 url
SLB-Switch(config-slb-map-url)# match protocol http url /index.html
SLB-Switch(config-slb-map-url)# match protocol http url /stocks/csco/
SLB-Switch(config-slb-map-url)# match protocol http url *gif
SLB-Switch(config-slb-map-url)# match protocol http url /st*
SLB-Switch(config-slb-map-url)# exit
SLB-Switch(config)
```

Related Commands

match protocol http url
url-map (SLB policy configuration submode)
show module csm map

match protocol http url

Use the **match protocol http url** command in the SLB URL map configuration submode to add a URL regular expression to a URL map. Multiple match rules can be added to a URL map. Use the **no** form of this command to remove the URL regular expression from the URL map.

match protocol http [**method** *method-expression*] **url** *url-expression*

no match protocol http url [**method** *method-expression*] **url** *url-expressionn*

Syntax Description

method	(Optional) Keyword to specify the method in incoming HTTP requests.
method-expression	Specifies the method expression to match.
url	Keyword to specify the URL in incoming HTTP requests.
url-expression	Regular expression range; the range is from 1 to 255 characters.

Defaults

This command has no default settings.

Command Modes

SLB URL map configuration submode.

Usage Guidelines

URL regular expressions are based on the UNIX filename specification. URL expressions are stored in a cookie map in the form *urln*. URL expressions do not allow spaces and only one of the URLs in the map must be matched.

"*" means zero or more characters

"?" means exactly one character—the [Ctrl + V] key combination must be entered

"\" means escaped character

Bracketed range (for example, [0–9]) means matching any single character from the range

A leading ^ in a range means don't match any in the range

".\a" means alert (ASCII 7)

".\b" means backspace (ASCII 8

".\f" means form-feed (ASCII 12)

".\n" means newline (ASCII 10)

".\r" means carriage return (ASCII 13)

".\t" means tab (ASCII 9)

".\v" means vertical tab (ASCII 11)

".\0" means null (ASCII 0)

".\\" means backslash

".\x##" means any ASCII character as specified in two-digit hexadecimal notation

The method expression may be either one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a string you specify that must be matched exactly (PROTOPLASM).

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	HTTP method parsing support was introduced.

Examples

This example shows how to adds URL expressions to a URL map:

```
SLB-Switch(config-slb-map-url)# match protocol http url Host header-value XYZ
```

Related Commands

map url
url-map (SLB policy configuration submode)
show module csm map

5323
D.

module csm

Use the **module csm** command to allow the association of load-balancing commands to a specific CSM module and enter the CSM module configuration submode for the specified slot. Use the **no** form of this command to remove the **module csm** configuration.

Note The **module ContentSwitching Module** *slot* command is the full syntax; the **module csm** *slot* command is a valid shortcut.

module csm *slot-number*

no module csm *slot-number*

Syntax Description

slot-number	Slot number where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Global configuration submode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Usage Guidelines

If you want to use the new multiple module configuration, you must change the **ip slb mode** command to **rp**. An existing CSM configuration is migrated to the new configuration when you change the mode from **csm** to **rp**. A prompt appears requesting a slot number. Migrating from a multiple module configuration to a single module configuration is supported. Migrating the Cisco IOS SLB configuration to the CSM configuration is not supported.

Examples

This example shows how to configure a CSM:

```
SLB-Switch(config)# module csm 5
SLB-Switch(config-module-csm)# vserver VS1
```

Related Commands

ip slb mode

natpool

Use the **natpool** command in module CSM configuration submode to configure NAT and create a client address pool. Use the **no** form of this command to remove a **natpool** configuration.

natpool *pool-name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *leading_1_bits*}

no natpool *pool-name*

Syntax Description

pool-name	Name of a client address pool; the character string is from 1 to 15 characters.
start-ip	Starting IP address that defines the range of addresses in the address pool.
end-ip	Ending IP address that defines the range of addresses in the address pool.
netmask	(Optional) Keyword to specify the subnet mask.
netmask	(Optional) Mask for the associated IP subnet.
prefix-length	(Optional) Keyword to specify the subnet mask.
leading_1_bits	(Optional) Mask for the associated IP subnet.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If you want to use client NAT, you must create at least one client address pool.

A maximum of 255 NAT pool addresses are available for any CSM.

Examples

This example shows how to configure a pool of addresses with the name **web-clients**, an IP address range from 128.3.0.1 through 128.3.0.254, and a subnet mask of 255.255.0.0:

```
SLB-Switch(config-module-csm)# natpool web-clients 128.3.0.1 128.3.0.254 netmask
255.255.0.0
```

Related Commands

nat client (SLB serverfarm configuration submode)
show module csm natpool

owner

Use the **owner** command in module CSM configuration submode to configure an owner object. Use the **no** form of this command to remove an **owner** configuration.

owner *name*

no owner

Syntax Description

name	Name of the object owner.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can define more than one virtual server with the same virtual IP address (VIP) and set the VIP connection watermark level to apply to a single VIP, which may correspond to multiple virtual servers. With the **owner** command, any virtual server has either zero or one owners. A particular owner can be associated with multiple virtual servers (typically, but not necessarily, with the same VIP). The VIP connection watermark applies to a specific owner. Once the sum of the number of open connections to all virtual servers in a particular owner reaches the VIP connection watermark level for that owner, new connections to any of these virtual servers are rejected by the CSM.

Examples

This example shows how to configure an owner object:

```
SLB-Switch(config-module-csm)# owner sequel
```

Related Commands

address
billing-info
contact-info
maxconns

address

Use the **address** command in the owner configuration submode to configure the address information for an owner object. Use the **no** form of this command to remove the address from the configuration.

address *street-address-information*

no address

Syntax Description

street-address-information	The owner's street address.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to configure an owner object:

```
SLB-Switch(config-owner)# address 125 marmalade street
```

Related Commands

owner
billing-info
contact-info

billing-info

Use the **billing-info** command in the owner configuration submode to configure billing information for an owner object. Use the **no** form of this command to remove an billing information from the configuration.

billing-info *billing-address-information*

no billing-info

Syntax Description

billing-info	Keyword to specify the owner's billing address.
billing-address-information	The owner's billing address.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to configure an owner object:

```
SLB-Switch(config-owner)# billing-info 300 cordera avenue
```

Related Commands

owner
address
contact-info

contact-info

Use the **contact-info** command in owner configuration submode to configure an email address for an owner object. Use the **no** form of this command to remove the contact information from the **owner** configuration.

contact-info *string*

no contact-info

Syntax Description

string	The owner's information.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to configure an owner object:

```
SLB-Switch(config-owner)# contact-info shaggy@angel.net
```

Related Commands

owner
address
billing-info

maxconns

Use the **maxconns** command in owner configuration submode to configure the maximum number of connections allowed for an owner object. Use the **no** form of this command to remove the maximum connections from the **owner** configuration.

maxconns *number*

no email-address

Syntax Description

number	The number of maximum connections to the owner object.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to configure an owner object:

```
SLB-Switch(config-owner)# maxconns 300
```

Related Commands

owner
address
billing-info
contact-info

policy

Use the **policy** command to configure policies, associate attributes to a policy, and enter the policy configuration submode. In this submode, you can configure the policy attributes. The policy is associated with a virtual server in virtual server submode. Use the **no** form of this command to remove a **policy**.

policy *policy-name*

no policy *policy-name*

Syntax Description

policy-name	Name of an slb-policy instance; the character string is limited to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
1(1)	This command was introduced.

Usage Guidelines

licies establish rules for balancing connections to servers. They can contain URL maps, cookie maps, ader maps, client groups, sticky groups, DSCP values, and server farms. The order in which policies linked to a virtual server determines the precedence of the policy. When two or more policies match equested URL, the policy with the highest precedence is selected.

u can create up to 12287 SLB policies for a given CSM module.

Note policies should be configured with a server farm.

Examples

example shows how to configure a policy named policy_content:

```
Switch(config-module-csm)# policy policy_content
Switch(config-slb-policy)# serverfarm new_serverfarm
Switch(config-slb-policy)# url-map url_map_1
Switch(config-slb-policy)# exit
```

Related Commands

licy (SLB virtual server configuration submode)
nodule csm owner

client-group

Use the **client-group** command in SLB policy configuration submode to associate an access list with the policy. Use the **no** form of this command to remove access list from the policy.

client-group {*1-99* | *std-access-list-name*}

no client-group

Syntax Description

1-99	Standard IP access list number.
std-access-list-name	Standard access list name.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode.

Command History

Release	**Modification**
1.1(1)	This command was introduced.

Usage Guidelines

Only client groups created with the **ip access-list standard** command can be associated with an SLB policy. Only one client-group can be associated with a given SLB policy.

Examples

This example shows how to configure a client group:

```
SLB-Switch(config-slb-policy)# client-group 44
SLB-Switch(config-slb-policy)# exit
```

Related Commands

policy
ip access-list standard
show module csm owner

cookie-map

Use the **cookie-map** command in SLB policy configuration submode to associate a list of cookies with a policy. Use the **no** form of this command to remove a cookie map.

cookie-map *cookie-map-name*

no cookie-map

Syntax Description

cookie-map-name	Name of the cookie list associated with a policy.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Only one cookie map can be associated with a policy. Cookie maps are configured using the **map cookie** command. The cookie map name must match the name specified in the **map cookie** command.

Examples

This example shows how to configure a cookie-based SLB policy named policy_content:

```
SLB-Switch(config-module-csm)# policy policy_content
SLB-Switch(config-slb-policy)# serverfarm new_serverfarm
SLB-Switch(config-slb-policy)# cookie-map cookie-map-1
SLB-Switch(config-slb-policy)# exit
SLB-Switch(config)
```

Related Commands

policy
map cookie
show module csm owner

header-map

Use the **header-map** command in SLB policy configuration submode to specify the HTTP header criteria to include in a policy. Use the **no** form of this command to remove a header map.

Note If any HTTP header information is matched, the policy rule is satisfied.

header-map *name*

no header-map

Syntax Description

name	Name of the previously configured HTTP header expression group.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Usage Guidelines

Only one header map can be associated with a policy. The header map name must match the name specified in the **map header** command on page A-18.

Examples

This example shows how to configure a header-based policy named policy_content:

```
SLB-Switch(config-module-csm)# policy policy_content
SLB-Switch(config-slb-policy)# serverfarm new_serverfarm
SLB-Switch(config-slb-policy)# header-map header-map-1
SLB-Switch(config-slb-policy)# exit
```

Related Commands

policy
map header
show module csm owner

reverse-sticky

Use the **reverse-sticky** command to ensure that the CSM switches connections in the opposite direction back to the original source. Use the **no** form of this command to remove the reverse-sticky option from the policy or the default-policy of a virtual server.

reverse-sticky *group-id*

no reverse-sticky

Syntax Description

group-id	Number identifying the sticky group to which the virtual server belongs; the range is from 0 to 255.

Defaults

The default is **no reverse-sticky**. Sticky connections are not tracked.
The group ID default is 0. The sticky feature is not used for other virtual servers.
The network default is 255.255.255.255.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The **IP reverse-sticky** command is introduced.

Examples

This example shows how to set the IP reverse-sticky feature:

```
SLB-Switch(config-module-csm)# vserver PUBLIC_HTTP
SLB-Switch(config-slb-vserver)# reverse-sticky 60
```

Related Commands

sticky
sticky-group (SLB policy submode)
show module csm sticky
show module csm vserver redirect

serverfarm

Use the **serverfarm** command in the SLB policy configuration submode to associate a server farm with a policy. Use the **no** form of this command to remove the server farm from the policy.

serverfarm *primary-serverfarm* [**backup** *sorry-serverfarm* [**sticky**]]

no serverfarm

Syntax Description

primary-serverfarm	Character string used to identify the server farm.
backup	(Optional) Keyword set the name of a backup serverfarm.
sorry-serverfarm	(Optional) Backup serverfarm name.
sticky	(Optional) Keyword to associate the backup serverfarm with a virtual server.

Defaults

This command has no default settings.

Command Modes

SLB policy configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The sorry server (backup server) option was added to this command.

Usage Guidelines

Use the **serverfarm** command to configure the server farm. Only one server farm can be configured per policy. The server farm name must match the name specified in the **serverfarm** module CSM configuration submode command. By default, the sticky option does not apply to the backup serverfarm. To remove the backup serverfarm, you can either use the serverfarm command without the backup option or use the **no serverfarm** command.

Examples

This example shows how to associate a server farm named central with a policy:

```
SLB-Switch(config-module-csm)# policy policy
SLB-Switch(config-slb-policy)# serverfarm central backup domino sticky
```

Related Commands

policy
reverse-sticky (module CSM configuration submode)
show module csm owner

5370
D.

set ip dscp

Use the **set ip dscp** command in the SLB policy configuration submode to mark packets that match the policy with a DSCP value. Use the **no** form of this command to stop marking packets.

set ip dscp *dscp-value*

no set ip dscp

Syntax Description

dscp-value	The range is from 0 to 63.

Defaults

The default is that the CSM does not store DSCP values.

Command Modes

SLB policy configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to mark packets to match a policy named policy_content:

```
SLB-Switch(config-module-csm)# policy policy_content
SLB-Switch(config-slb-policy)# set ip dscp 22
```

Related Commands

policy
show module csm owner

sticky-group

Use the **sticky-group** command in the SLB policy configuration submode to associate a sticky group and the sticky group attributes to the policy. Use the **no** form of this command to remove the sticky group from the policy.

sticky-group *group-id*

no sticky-group

Syntax Description

group-id	ID of the sticky group to be associated with a policy.

Defaults

The default is 0, which means that no connections are sticky.

Command Modes

SLB policy configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The *group-id* must match the ID specified in the **sticky** command; the range is from 1 to 255.

Examples

This example shows how to configure a sticky group:

```
SLB-Switch(config-module-csm)# policy policy1
SLB-Switch(config-slb-policy)# sticky-group 5
```

Related Commands

policy
sticky
show module csm owner
show module csm sticky

5968 D

url-map

Use the **url-map** command in SLB policy configuration submode to associate a list of URLs with the policy. Use the **no** form of this command to remove the URL map from the policy.

url-map *url-map-name*

no url-map

Syntax Description

url-map-name	Name of the URL list to be associated with a policy.

Defaults

The default is no URL map.

Command Modes

SLB policy configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Only one URL map can be associated with a policy. URL maps are configured using the **map url** command.

Examples

This example shows how to associate a list of URLs with a policy named assembly:

```
SLB-Switch(config-module-csm)# policy policy
SLB-Switch(config-slb-policy)# url-map assembly
```

Related Commands

policy
map url
show module csm owner

probe

Use the **probe** command to configure a probe and probe type for health monitoring and to enter the probe configuration submode. Use the **no** form of this command to remove a probe from the configuration.

probe *probe-name* {**http** | **icmp** | **telnet** | **tcp** | **ftp** | **smtp** | **dns** | **kal-ap-upd**}

no probe *probe-name*

Syntax Description

probe-name	Name of the probe; the character string is limited to 15 characters.
http	Keyword to create an HTTP probe with a default configuration.
icmp	Keyword to create an ICMP probe with a default configuration.
telnet	Keyword to create a Telnet probe with a default configuration.
tcp	Keyword to create a TCP probe with a default configuration.
ftp	Keyword to create an FTP probe with a default configuration.
smtp	Keyword to create an SMTP probe with a default configuration.
dns	Keyword to create a DNS probe with a default configuration.
kal-ap-udp	Keyword to create a GSLB target probe.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

A probe can be assigned to a server farm in serverfarm submode.

When configuring kal-ap-udp type probes, the **port** submode command is not used to specify the destination UDP port to query. Use theCSM environment variable GSLB_KALAP_UDP_PORT instead. The default is port 5002.

Also, to specify probe frequency and the number of retries for KAL-AP, ICMP, HTTP and DNS probes when associated with a GSLB serverfarm environment, the following variables must be used instead of the probe submode commands:

```
GSLB_KALAP_PROBE_FREQ          10
GSLB_KALAP_PROBE_RETRIES       3
GSLB_ICMP_PROBE_FREQ           10
GSLB_ICMP_PROBE_RETRIES        3
GSLB_HTTP_PROBE_FREQ           10
GSLB_HTTP_PROBE_RETRIES        2
GSLB_DNS_PROBE_FREQ            10
GSLB_DNS_PROBE_RETRIES         3
```

5966
D

Examples

This example shows how to configure an HTTP probe named TREADER:

```
SLB-Switch(config-module-csm)# probe TREADER http
```

Related Commands

probe (SLB serverfarm configuration submode)
show module csm probe

address (dns)

Use the **address** command in SLB DNS probe configuration submode to specify an IP address of the real server used by DNS to resolve requests. Use the **no** form of this command to remove the address.

address *ip-address*

no address *ip-address*

Syntax Description

ip-address	Real server IP address.

Defaults

This command has no default settings.

Command Modes

SLB DNS probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Multiple addresses can be configured for a DNS probe.

Examples

This example shows how to configure an IP address of the DNS server:

```
SLB-Switch(config-slb-probe-dns)# address 101.23.45.36
```

Related Commands

probe
address (icmp)
show module csm probe

address (icmp)

Use the **address** command in SLB ICMP probe configuration submode to specify a destination IP address for health monitoring. Use the **no** form of this command to remove the address.

address *ip-address*

no address

Syntax Description

ip-address	Real server IP address.

Defaults

This command has no default settings.

Command Modes

SLB ICMP probe configuration submode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Usage Guidelines

One address can be configured for an ICMP probe.

Examples

This example shows how to configure an IP address of the real server:

```
SLB-Switch(config-slb-probe-icmp)# address 101.23.45.36
```

Related Commands

probe
address (dns)
show module csm probe

credentials

Use the **credentials** command in the SLB HTTP probe configuration submode to configure basic authentication values for an HTTP probe. Use the **no** form of this command to remove the credentials configuration.

credentials *username* [*password*]

no credentials

Syntax Description

username	Name that appears in the HTTP header.
password	(Optional) Password that appears in the HTTP header.

Defaults

This command has no default settings.

Command Modes

SLB HTTP probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is for HTTP probes.

Examples

This example shows how to configure authentication for an HTTP probe:

```
SLB-Switch(config-slb-probe-http)# credentials seamless abercrombie
```

Related Commands

probe
show module csm probe

expect status

Use the **expect status** command in the SLB HTTP/FTP/Telnet/SMTP probe configuration submode to configure a status code for the probe. Use the **no** form of this command to remove the status code from the configuration.

expect status *min-number* [*max-number*]

no expect status *min-number* [*max-number*]

Syntax Description

min-number	Single status code if *max-number* is not specified.
max-number	(Optional) Maximum status code in a range.

Defaults

The default range is 0 to 999 (any response from the server is valid). Both min-number and max-number can be any number between 0 and 999, as long as max-number is not lower than min-number.

For example:

`expect status 5` is the same as `expect status 5 5`

`expect status 0` specifies a range of 0 to 4

`expect status 900 999` specifies a range of 900 to 999.

You can specify many expected status ranges.

Command Modes

SLB HTTP/FTP/Telnet/SMTP probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is for HTTP, FTP, Telnet, and SMTP probes. You can specify multiple status code ranges with this command by entering one command at a time. If you specify the *max-number* value, this number is used as the minimum status code of a range. If you specify no maximum number, this command uses a single number (*min-number*). If you specify both *min-number* and *max-number* values, this command uses the range between the numbers.

Note When you remove the expect status, you cannot set the range of numbers to 0 or as a range of numbers that includes the values you set for the expect status. The expect status state becomes invalid and does not restore the default range of 0 through 999. To remove the expect status, remove each set of numbers using the **no expect status** command. For example, enter the **no expect status 0 3** command and then enter the **no expect status 34 99** command.

Examples

This example shows how to configure an HTTP probe with multiple status code ranges:

```
SLB-Switch(config-slb-probe-http)# expect status 34 99
SLB-Switch(config-slb-probe-http)# expect status 0 33
SLB-Switch(config-slb-probe-http)#
```

Related Commands

probe
show module csm probe

5960
D.

failed

Use the **failed** command in the SLB probe configuration submode to set the time to wait before probing a failed server. Use the **no** form of this command to reset the time to wait before probing a failed server to default.

failed *failed-interval*

no failed

Syntax Description

failed-interval	Time in seconds before retrying a failed server; the range is from 2 to 65535.

Defaults

The default value for the failed interval is 300 seconds.

Command Modes

SLB probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Examples

This example shows how to configure a failed server probe for 200 seconds:

```
SLB-Switch(config-slb-probe-http)# failed 200
```

Related Commands

probe
show module csm probe

header

Use the **header** command in the SLB HTTP probe configuration submode to configure a header field for the HTTP probe. Use the **no** form of this command to remove the credentials configuration.

header *field-name* [*field-value*]

no header *field-name*

Syntax Description

field-name	Name for the header being defined.
field-value	(Optional) Content for the header.

Defaults

This command has no default settings.

Command Modes

SLB HTTP probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can configure multiple headers for each HTTP probe. The length of the *field-name* value plus the length of the *field-value* value plus 4 (for ":", space, and CRLF) cannot exceed 255 characters. This command is for HTTP probes.

Examples

This example shows how to configure a header field for the HTTP probe:

```
SLB-Switch(config-slb-probe-http)# header abacadabra
```

Related Commands

probe
show module csm probe

5958
D

interval

Use the **interval** command in the SLB probe configuration submode to set the time interval between probes. Use the **no** form of this command to reset the time interval between probes to default.

interval *seconds*

no interval

Syntax Description

seconds	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe; the range is from 2 to 65535.

Defaults

The default value for the interval between probes is 120 seconds.

Command Modes

SLB probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Examples

This example shows how to configure a probe interval of 150 seconds:

```
SLB-Switch(config-slb-probe-http)# interval 150
```

Related Commands

probe
show module csm probe

kal-ap-udp

Use the **kal-ap-udp** command in the SLB probe configuration submode to set a probe for a Global Server Load Balancing (GSLB) target for load information. Use the **no** form of this command to remove the GSLB probe.

kal-ap-udp *seconds*

no kal-ap-udp

Syntax Description

seconds	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe; the range is from 2 to 65535.

Defaults

The default value for the interval between probes is 120 seconds.

Command Modes

SLB probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Examples

This example shows how to configure a probe interval of 150 seconds:

```
SLB-Switch(config-slb-probe-http)# interval 150
```

Related Commands

probe
show module csm probe

name

Use the **name** command in the SLB DNS probe configuration submode to configure a domain name for the DNS probe. Use the **no** form of this command to remove the name from the configuration.

name *domain-name*

no name

Syntax Description

domain-name	Domain name that the probe sends to the DNS server.

Defaults

This command has no default settings.

Command Modes

SLB DNS probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify the probe name that is resolved by the DNS server:

```
SLB-Switch(config-slb-probe-dns)# name astro
```

Related Commands

probe
show module csm probe

port

Use the **port** command in the SLB probe configuration submode to configure an optional port for the DNS probe. Use the **no** form of this command to remove the port from the configuration.

port *port-number*

no port

Syntax Description

port-number	Sets the port number.

Defaults

The default value for the port number is 0.

Command Modes

This command is available in all SLB probe configuration submodes except ICMP.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When the port of a health probe is specified as 0, the health probe uses the configured port number from the real server (if a real server is configured) or the configured port number from the virtual server (if a virtual server is configured and no port is configured for the real server). The default port value is 0. For the ICMP probes, where there is no port number, the port value is ignored. The **port** command is available for all probe types except ICMP.

Examples

This example shows how to specify the port for the DNS server:

```
SLB-Switch(config-slb-probe-dns)# port 63
```

Related Commands

probe
show module csm probe

59SH

D.

open

Use the **open** command in the SLB HTTP/TCP/FTP/Telnet/SMTP probe configuration submode to set the time to wait for a TCP connection. Use the **no** form of this command to reset the time to wait for a TCP connection to default.

open *open-timeout*

no open

Syntax Description

open-timeout	Maximum number of seconds to wait for the TCP connection; the range is from 1 to 65535.

Defaults

The default value for the open timeout is 10 seconds.

Command Modes

SLB HTTP/TCP/FTP/Telnet/SMTP probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is not used for any non-TCP probes, for example, ICMP or DNS.

Note There are two different timeout values: open and receive. The open timeout specifies how many seconds to wait for the connection to open (that is, how many seconds to wait for SYN ACK after sending SYN). The receive timeout specifies how many seconds to wait for data to be received (that is, how many seconds to wait for an HTTP reply after sending a GET/HHEAD request). Because TCP probes close as soon as they open without sending any data, the receive timeout is not used.

Examples

This example shows how to configure a time to wait for a TCP connection of 5 seconds:

```
SLB-Switch(config-slb-probe-http)# open 5
```

Related Commands

probe
show module csm probe

receive

Use the **receive** command in the SLB probe configuration submode to set the time to wait for a reply from a server. Use the **no** form of this command to reset the time to wait for a reply from a server to default.

receive *receive-timeout*

no receive

Syntax Description

receive-timeout	Number of seconds to wait for reply from a server; the range is from 1 to 65535.

Defaults

The default value for a receive timeout is 10 seconds.

Command Modes

SLB probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is available for all probe types, except TCP.

Note There are two different timeout values: open and receive. The open timeout specifies how many seconds to wait for the connection to open (that is, how many seconds to wait for SYN ACK after sending SYN). The receive timeout specifies how many seconds to wait for data to be received (that is, how many seconds to wait for an HTTP reply after sending a GET/HHEAD request). Because TCP probes close as soon as they open without sending any data, the receive timeout is not used.

Examples

This example shows how to configures a time to wait for a reply from a server to 5 seconds:

```
SLB-Switch(config-slb-probe-http)# receive 5
```

Related Commands

probe
show module csm probe

5962
D

request

Use the **request** command in the SLB HTTP probe configuration submode to configure the request method used by the HTTP probe. Use the **no** form of this command to remove the request method from the configuration.

request [method {get | head}]] [url *path***]**

no request [method {get | head}] [url *path***]**

Syntax Description

method	(Optional) Keyword to configure a method for the probe request.
get	(Optional) Keyword to direct the server to get this page.
head	(Optional) Keyword to direct the server to get only the header for this page.
url	(Optional) Keyword to direct the server to get the URL for this page.
path	(Optional) A character string up to 255 characters specifying the URL path.

Defaults

The default path is /.
The default method is **get**.

Command Modes

SLB HTTP probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The CSM supports only the **get** and **head** request methods. It does not support **post** and other methods. This command is for HTTP probes.

Examples

This example shows how to configure a request method for the probe configuration:

```
SLB-Switch(config-slb-probe-http)# request method head
```

Related Commands

probe
show module csm probe

retries

Use the **retries** command in the SLB probe configuration submode to set the number of failed probes that are allowed before marking the server failed. Use the **no** form of this command to reset the number of failed probes allowed before marking a server as failed to default.

retries *retry-count*

no retries

Syntax Description

retry-count	Number of probes to wait before marking a server as failed; the range is from 0 to 65535.

Defaults

The default value for retries is 3.

Command Modes

SLB probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Note Set retries to 2 or more. If retries are set to 1, a single dropped probe packet will bring down the server. A setting of 0 places no limit on the number of probes that are sent. Retries are sent until the system reboots.

Examples

This example shows how to configure a retry count of 3:

```
SLB-Switch(config-slb-probe-http)# retries 3
```

Related Commands

probe
show module csm probe

5959

D

probe script

Use the **probe** *probe-name* **script** command to create a script probe and enter the probe script configuration submode. Use the **no** form of this command to remove the probe from the configuration.

probe *probe_name* **script**

no probe *probe_name* **script**

Syntax Description

probe_name	Names the probe script
script	Keyword that specifies the creation of a probe script.

Defaults

This command has no default settings.

Command Modes

SLB probe script configuration submode.

Usage Guidelines

This command enters a probe sub-mode that is similar to the existing CSM health probe sub-modes (such as HTTP, TCP, DNS, and SMTP). The script probe sub-mode contains the existing probe sub-mode commands **failed, interval, open, receive,** and **retries.**

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to create a script probe:

```
SLB-Switch(config-module-csm)# ip slb script file tftp://192.168.10.102/csmScripts
SLB-Switch(config-probe-script)# script echoProbe.tcl
SLB-Switch(config-probe-script)# interval 10
SLB-Switch(config-probe-script)# retries 1
SLB-Switch(config-probe-script)# failed 30
```

Related Commands

probe
script, page A-63
failed, page A-64
interval, page A-65
open, page A-66
receive, page A-67
retries, page A-68
show module csm probe

script

Use the **script** *script-name* **[arg1 [arg2...]]** command to create a script probe. Use the **no** form of this command to remove the probe from the configuration.

script *script_name* **[arg1 [arg2...]]**

no script *script_name* **[arg1 [arg2...]]**

Syntax Description

script-name	Names the probe script
arg1, arg2	Keyword that specifies ???

Defaults

This command has no default settings.

Command Modes

SLB probe script configuration submode.

Usage Guidelines

This command enters a probe sub-mode that is similar to the existing CSM health probe sub-modes (such as HTTP, TCP, DNS, and SMTP). The script probe sub-mode contains the existing probe sub-mode commands failed, interval, open, receive, and retries.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to create a script probe:

```
SLB-Switch(config-module-csm)# ip slb script file tftp://192.168.10.102/csmScripts
SLB-Switch(config-probe-script# script echoProbe.tcl
SLB-Switch(config-probe-script# interal 10
SLB-Switch(config-probe-script# retries 1
SLB-Switch(config-probe-script# failed 30
```

Related Commands

probe
failed, page A-64
interval, page A-65
open, page A-66
receive, page A-67
retries, page A-68
show module csm probe

failed

Use the **failed** command in the SLB probe scirpt configuration submode to set the time to wait before probing a failed server. Use the **no** form of this command to reset the time to wait before probing a failed server to default.

failed *failed-interval*

no failed

Syntax Description

failed-interval	Time in seconds before retrying a failed server; the range is from 2 to 65535.

Defaults

The default value for the failed interval is 300 seconds.

Command Modes

SLB probe script configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Examples

This example shows how to configure a failed server probe for 200 seconds:

```
SLB-Switch(config-slb-probe-http)# failed 200
```

Related Commands

probe
script, page A-63
interval, page A-65
open, page A-66
receive, page A-67
retries, page A-68
show module csm probe

interval

Use the **interval** command in the SLB probe script configuration submode to set the time interval between probes. Use the **no** form of this command to reset the time interval between probes to default.

interval *seconds*

no interval

Syntax Description

seconds	Number of seconds to wait between probes from the end of the previous probe to the beginning of the next probe; the range is from 2 to 65535.

Defaults

The default value for the interval between probes is 120 seconds.

Command Modes

SLB probe script configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Examples

This example shows how to configure a probe interval of 150 seconds:

```
SLB-Switch(config-slb-probe-http)# interval 150
```

Related Commands

probe
script, page A-63
failed, page A-64
open, page A-66
receive, page A-67
retries, page A-68
show module csm probe

5946

open

OPL

Use the **open** command in the SLB probe script configuration submode to set the time to wait for a reply from a server. Use the **no** form of this command to reset the time to wait for a reply from a server to default.

open *open-timeout*

no open

Syntax Description

open-timeout	Number of seconds to wait for reply from a server; the range is from 1 to 65535.

Defaults

The default value for a receive timeout is 10 seconds.

Command Modes

SLB probe script configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is available for all probe types, except TCP.

Note There are two different timeout values: open and receive. The open timeout specifies how many seconds to wait for the connection to open (that is, how many seconds to wait for SYN ACK after sending SYN). The receive timeout specifies how many seconds to wait for data to be received (that is, how many seconds to wait for an HTTP reply after sending a GET/HHEAD request). Because TCP probes close as soon as they open without sending any data, the receive timeout is not used.

Examples

This example shows how to configures a time to wait for a reply from a server to 5 seconds:

```
SLB-Switch(config-slb-probe-http)# open 5
```

Related Commands

probe
script, page A-63
failed, page A-64
interval, page A-65
receive, page A-67
retries, page A-68
show module csm probe

5945
D

receive

Use the **receive** command in the SLB probe configuration submode to set the time to wait for a reply from a server. Use the **no** form of this command to reset the time to wait for a reply from a server to default.

receive *receive-timeout*

no receive

Syntax Description

receive-timeout	Number of seconds to wait for reply from a server; the range is from 1 to 65535.

Defaults

The default value for a receive timeout is 10 seconds.

Command Modes

SLB probe configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is available for all probe types, except TCP.

Note There are two different timeout values: open and receive. The open timeout specifies how many seconds to wait for the connection to open (that is, how many seconds to wait for SYN ACK after sending SYN). The receive timeout specifies how many seconds to wait for data to be received (that is, how many seconds to wait for an HTTP reply after sending a GET/HHEAD request). Because TCP probes close as soon as they open without sending any data, the receive timeout is not used.

Examples

This example shows how to configures a time to wait for a reply from a server to 5 seconds:

```
SLB-Switch(config-slb-probe-http)# receive 5
```

Related Commands

probe
script, page A-63
failed, page A-64
interval, page A-65
open, page A-66
retries, page A-68
show module csm probe

5944
D

retries

Use the **retries** command in the SLB probe script configuration submode to set the number of failed probes that are allowed before marking the server failed. Use the **no** form of this command to reset the number of failed probes allowed before marking a server as failed to default.

retries *retry-count*

no retries

Syntax Description

retry-count	Number of probes to wait before marking a server as failed; the range is from 0 to 65535.

Defaults

The default value for retries is 3.

Command Modes

SLB probe script configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command is used for all probe types.

Note Set retries to 2 or more. If retries are set to 1, a single dropped probe packet will bring down the server. A setting of 0 places no limit on the number of probes that are sent. Retries are sent until the system reboots.

Examples

This example shows how to configure a retry count of 3:

```
SLB-Switch(config-slb-probe-script)# retries 3
```

Related Commands

probe
script, page A-63
failed, page A-64
interval, page A-65
open, page A-66
receive, page A-67
show module csm probe

real

Use the **real** command in the SLB serverfarm configuration submode to identify a real server that is a member of the server farm and enter the real server configuration submode. Use the **no** form of this command to remove the real server from the configuration.

real *ip-address* [*port*]

no real *ip-address* [*port*]

Syntax Description

ip-address	Real server IP address.
port	(Optional) Port translation for the real server; the range is from 1 to 65535.

Defaults

The default is no port translation for the real server.

Command Modes

SLB serverfarm configuration submode.

Usage Guidelines

Use this command to identify a real server that is a member of the server farm and enter the real server configuration submode.

Note The IP address that you supply provides a load-balancing target for the CSM. This target can be any IP addressable object. For example, the IP addressable object may be a real server, a firewall, or an alias IP address of another CSM.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to identify a real server and enter the real server submode:

```
SLB-Switch(config-slb-sfarm)# real 102.43.55.60
SLB-Switch(config-slb-real)#
```

Related Commands

serverfarm
show module csm real
show module csm serverfarm

S942
D.

inservice

Use the **inservice** command in the SLB real server configuration submode to enable the real servers. Use the **no** form of this command to remove a real server from service.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Defaults

The default for a real server is **no inservice**.

Command Modes

SLB real server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to enable a real server:

```
SLB-Switch(config-slb-sfarm)# real 10.2.2.1
SLB-Switch(config-slb-real)# inservice
```

Related Commands

real (SLB serverfarm submode)
show module csm real

maxconns

Use the **maxconns** command in the SLB real server configuration submode to limit the number of active connections to the real server. Use the **no** form of this command to change the maximum number of connections to its default value.

maxconns *max-conns*

no maxconns

Syntax Description

max-conns	Maximum number of active connections on the real server at any one point in time; the range is from 1 to 4294967295.

Defaults

The default value is the maximum value or infinite (not monitored).

Command Modes

SLB real server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When you specify **minconns**, you must also specify the **maxconns** command.

Examples

This example shows how to limit the connections to a real server:

```
SLB-Switch(config-slb-sfarm)# real 10.2.2.1
SLB-Switch(config-slb-real)# maxconns 4000
```

Related Commands

minconns (real server submode)
real (serverfarm submode)
show module csm real

5940
D.

minconns

Use the **minconns** command in the SLB real server configuration submode to establish a minimum connection threshold for the real server. Use the **no** form of this command to change the minimum number of connections to the default value.

minconns *min-cons*

no minconns

Syntax Description

min-cons	Minimum number of connections allowed on the real server; the range is from 0 to 4294967295.

Defaults

The default value is **no minconns**.

Command Modes

SLB real server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When the **maxconns** threshold is exceeded, the CSM stops sending connections until the number of connections falls below the **minconns** threshold. This value must be lower than the maximum number of connections configured by the **maxconns** command. When you specify **minconns**, you must also specify the **maxconns** command.

Examples

This example shows how to establish a minimum connection threshold for a server:

```
SLB-Switch(config-slb-sfarm)# real 102.2.2.1
SLB-Switch(config-slb-real)# minconns 4000
```

Related Commands

maxconns (real server submode)
real (serverfarm submode)
show module csm real

probe

Use the **probe** command in the SLB real server configuration submode to configure a probe for the real server. Use the **no** form of this command to remove the probe from the configuration.

probe *probe-name* **tag** *string*

no probe

Syntax Description

probe-name	Names the probe.
tag	Keyword to specify a tag for the probe.
string	Specifies a string to identify the probe.

Defaults

This command has no default values.

Command Modes

SLB real server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to configurre a probe for a server:

```
SLB-Switch(config-slb-sfarm)# real 102.2.2.1
SLB-Switch(config-slb-real)# probe mission tag 12345678
```

Related Commands

real (serverfarm submode)
show module csm real

redirect-vserver

Use the **redirect-vserver** command in the SLB real server configuration submode to configure a real server to receive traffic redirected by a redirect virtual server. Use the **no** form of this command to specify that traffic is not redirected to the real server.

redirect-vserver *name*

no redirect-vserver

Syntax Description

name	Name of the virtual server that has its requests redirected.

Defaults

The default is **no redirect-vserver**.

Command Modes

SLB real server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Mapping real servers to redirect virtual servers provides persistence for clients to real servers across TCP sessions. Before using this command, you must create the redirect virtual server in serverfarm submode with the **redirect-vserver** command.

Examples

This example shows how to map a real server to a virtual server:

```
SLB-Switch(config-slb-sfarm)#   real 10.2.2.1
SLB-Switch(config-slb-real)# redirect-vserver timely
```

Related Commands

real (SLB serverfarm configuration submode)
redirect-vserver (SLB serverfarm configuration submode)
show module csm real
show module csm vserver redirect

weight

Use the **weight** command in the SLB real server configuration submode to configure the capacity of the real servers in relation to the other real servers in the server farm. Use the **no** form of this command to change the server's weight to its default capacity.

weight *weighting-value*

no weight

Syntax Description

weighting-value	Value to use for the server farm predictor algorithm; the range is from 1 to 100.

Defaults

The weighting value default is 8.

Command Modes

SLB real server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to configure the weight of a real server:

```
SLB-Switch(config-slb-sfarm)#   real 10.2.2.1
SLB-Switch(config-slb-real)# weight 8
```

Related Commands

predictor (SLB serverfarm submode)
real (SLB serverfarm submode)
show module csm real

5936
D

redirect-vserver

Use the **redirect-vserver** command to specify the name of a virtual server to receive traffic redirected by the server farm and enter redirect virtual server configuration submode. Use the **no** form of this command to remove the redirect virtual server.

redirect-vserver *name*

no redirect-vserver *name*

Syntax Description

name	Name of the virtual server to receive traffic redirected by the server farm; the virtual server name can be no longer than 15 characters.

Defaults

This command has no default settings.

Command Modes

SLB serverfarm configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to name the virtual server:

```
SLB-Switch(config-slb-sfarm)#   redirect-vserver quantico
```

Related Commands

real (SLB serverfarm submode)
redirect-vserver (SLB real server submode)
serverfarm
show module csm serverfarm
show module csm vserver redirect

advertise

Use the **advertise** command in the SLB redirect virtual server configuration mode to allow the CSM to advertise the IP address of the virtual server as host-route. Use the **no** form of this command to stop advertising the host-route for this virtual server.

advertise [**active**]

no advertise

Syntax Description

active	(Optional) Keyword to allow the CSM to advertise the IP address of the virtual server as host-route.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB redirect virtual server configuration submode.

Usage Guidelines

Without the active option, the CSM always advertises the virtual server IP address whether or not there is any active real server attached to this virtual server.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to restrict a client from using the redirect virtual server:

```
SLB-Switch(config-slb-redirect-vs)# advertise 10.5.2.1 exclude
```

Related Commands

vserver
show module csm vserver redirect

client

Use the **client** command in the SLB redirect virtual server configuration mode to restrict which clients are allowed to use the redirect virtual server. Use the **no** form of this command to remove the client definition from the configuration.

client *ip-address* [*network-mask*] [**exclude**]

no client *ip-address* [*network-mask*]

Syntax Description

ip-address	Client's IP address.
network-mask	(Optional) Client's IP mask.
exclude	(Optional) Keyword to specify that the IP address is disallowed.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB redirect virtual server configuration submode.

Usage Guidelines

The network mask is applied to the source IP address of incoming connections and the result must match the IP address before the client is allowed to use the virtual server. If you do not specify exclude, the IP address and network mask combination is allowed.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to restrict a client from using the redirect virtual server:

```
SLB-Switch(config-slb-redirect-vs)# client 10.5.2.1 exclude
```

Related Commands

client-group (SLB policy submode)
vserver
show module csm vserver redirect

idle

Use the **idle** command in the SLB redirect virtual server configuration submode to specify the connection idle timer duration. Use the **no** form of this command to disable the idle timer.

idle *duration*

no idle

Syntax Description

duration	SLB connection idle timer in seconds; the range is from 4 to 65535.

Defaults

The default is 3600.

Command Modes

SLB redirect virtual server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify the connection idle timer duration:

```
SLB-Switch(config-slb-redirect-vs)# idle 7
```

Related Commands

redirect-vserver (SLB serverfarm submode)
show module csm vserver redirect

5832
D

inservice

Use the **inservice** command in the SLB redirect virtual server configuration submode to enable the real server for use by the CSM. If this command is not specified, the virtual server is defined but not used. Use the **no** form of this command to disable the virtual server.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Defaults

The default is **no inservice**.

Command Modes

SLB redirect virtual server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to enable a redirect virtual server for use by the CSM:

```
SLB-Switch(config-slb-redirect-vs)# inservice
```

Related Commands

redirect-vserver (SLB serverfarm submode)
show module csm vserver redirect

replicate csrp

Use the **replicate csrp** command in the SLB redirect virtual server configuration submode to enable connection redundancy. Use the **no** form of this command to remove connection redundancy.

replicate csrp

no replicate csrp

Syntax Description

This command has no keywords or arguments.

Defaults

The default is **no replicate csrp**.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to enable connection redundancy:

```
SLB-Switch(config-slb-redirect-vs)# replicate csrp
```

Related Commands

vserver
show module csm vserver redirect

5930

ssl

Use the **ssl** command in the SLB redirect virtual server configuration submode to redirect an HTTP request to either HTTPS (SSL)_ or the FTP service. Use the **no** form of this command to reset the redirect of an HTTP request to an HTTP service.

ssl {**https** | **ftp** | *ssl-port-number*}

no ssl

Syntax Description

ssl-port-number	SSL port number; the range is from 1 to 65535.

Defaults

The default is **no ssl** forwarding.

Command Modes

SLB redirect virtual server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to enable SSL forwarding:

```
SLB-Switch(config-slb-redirect-vs)# ssl 443
```

Related Commands

redirect-vserver (SLB serverfarm submode)
show module csm vserver redirect

virtual

Use the **virtual** command in SLB redirect virtual server configuration submode to specify the virtual server's IP address, the protocol used for traffic, and the port the protocol is using. Use the **no** form of this command to reset the virtual server to its defaults.

virtual *v_ipaddress* **tcp** *port*

no virtual *v_ipaddress*

Syntax Description

v_ipaddress	Redirect virtual server's IP address.
tcp	Keyword to specify the protocol used for redirect virtual server traffic.
port	Port number used by the protocol.

Defaults

The default IP address is 0.0.0.0, which prevents packet forwarding.

Command Modes

SLB redirect virtual server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify the virtual server's IP address, the protocol for redirect virtual server traffic, and the port number used by the protocol:

```
SLB-Switch(config-slb-redirect)# virtual 130.32.44.50 tcp 80
```

Related Commands

redirect-vserver (SLB serverfarm submode)
show module csm vserver redirect

vlan

5928

Use the **vlan** command in the SLB redirect virtual server submode to define which source VLANs can be accessed on the redirect virtual server. Use the **no** form of this command to remove the VLAN.

vlan {*vlan-number* | **all**}

no vlan

Syntax Description

vlan-number	VLAN the virtual server may access.
all	(Optional) Keyword to specify all VLANs are accessed by the virtual server.

Defaults

The default is all VLANs.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to specify a VLAN for redirect virtual server access:

```
SLB-Switch(config-slb-redirect-vs)# vlan 5
```

Related Commands

sticky
sticky-group (SLB policy submode)
show module csm sticky
show module csm vserver redirect

webhost backup

Use the **webhost backup** command in SLB redirect virtual server configuration submode to specify a backup string sent in response to HTTP requests. Use the **no** form of this command to disable the backup string.

webhost backup *backup-string* **[301 | 302]**

webhost backup

Syntax Description

backup-string	String sent in response to redirected HTTP requests; the maximum length is 127 characters.
301	(Optional) Keyword to specify the HTTP status code: "The requested resource has been assigned a new permanent URL."
302	(Optional) Keyword to specify the HTTP status code: "The requested resource resides temporarily under a different URL."

Defaults

The default status code is 302.

Command Modes

SLB redirect virtual server configuration submode.

Usage Guidelines

This command is used in situations where the redirect virtual server has no available real servers. **301** or **302** is used to specify the redirect code. The backup string may include a %p at the end to indicate inclusion of the path in the HTTP redirect location statement field.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify a backup string that is sent in response to HTTP requests:

```
SLB-Switch(config-slb-redirect-vs)# webhost backup www.mybackup.com%p 301
```

Related Commands

redirect-vserver (SLB serverfarm submode)
show module csm vserver redirect

webhost relocation

Use the **webhost relocation** command in the SLB redirect virtual server configuration submode to specify a relocation string sent in response to HTTP requests. Use the **no** form of this command to disable the relocation string.

webhost relocation *relocation string* [**301** | **302**]

no webhost relocation

Syntax Description

relocation string	String sent in response to redirected HTTP requests; the maximum length is 127 characters.
301	(Optional) Keyword to specify the HTTP status code: "The requested resource has been assigned a new permanent URL."
302	(Optional) Keyword to specify the HTTP status code: "The requested resource resides temporarily under a different URL."

Defaults

The default status code is 302.

Command Modes

SLB redirect virtual server configuration submode.

Usage Guidelines

The backup string may include a %p at the end to indicate inclusion of the path in the HTTP redirect location statement field.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify a relocation string that is sent in response to HTTP requests:

```
SLB-Switch(config-slb-redirect-vs)# webhost relocation www.myhome1.com%p 301
```

Related Commands

redirect-vserver (SLB serverfarm submode)
show module csm vserver redirect

script file

Use the **script file** command to load scripts into a script file. Use the **no** form of this command to remove the script file command from the configuration.

script file *file-url*

no script file

Syntax Description

file-url	Sets the standard Cisco IOS file name, such as *bootflash:webprobe.tcl*.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Usage Guidelines

The file-url is a standard Cisco IOS file name such as *bootflash:webprobe.tcl*.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to load scripts into a script file:

```
SLB-Switch(config-module-csm)# script file file-url
```

Related Commands

show module csm script

script task

Use the **script task** command to run a standalone task. Use the **no** form of this command to remove the standalone task from the configuration.

script task *script-index script-name* [**arg1** [**arg2...**]]

no script task *script-index*

Syntax Description

script-index	Used to identify a specific running script. The *script-index* is an integer between 1 and 100.
script-name	Identifies the script by name.
arg1, arg2	(Optoinal) Arguments can be any string to a particular script.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to run a standalone script:

```
SLB-Switch(config-module-csm)# script task 30 filerun
```

Related Commands

show module csm script

serverfarm

Use the **serverfarm** command to identify a server farm and enter the serverfarm configuration submode. Use the **no** form of this command to remove the server farm from the configuration.

serverfarm *serverfarm-name*

no serverfarm *serverfarm-name*

Syntax Description

serverfarm-name	Character string used to identify the server farm; the character string is limited to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Usage Guidelines

Use this command to enter the server farm configuration submode to configure the load-balancing algorithm (predictor), a set of real servers, and the attributes (NAT, probe, and bindings) of the real servers.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to identify a server farm named PUBLIC and change the CLI to server farm configuration mode:

```
SLB-Switch(config-module-csm)#   serverfarm PUBLIC
```

Related Commands

reverse-sticky (SLB policy configuration submode)
serverfarm (SLB virtual server configurations submode)
show module csm serverfarm

bindid

Use the **bindid** command in the SLB serverfarm configuration submode to assign a unique ID to allow the DFP agent to differentiate a real server in one server farm versus another server farm. Use the **no** form of this command to disable the bindid.

bindid [*bind-id*]

no bindid

Syntax Description

bind-id	(Optional) Identification number for each binding; the range is from 0 to 65533.

Defaults

The default is 0.

Command Modes

SLB serverfarm configuration submode.

Usage Guidelines

The single real server is represented as multiple instances of itself, each having a different bind identification. DFP uses this identification to identify a given weight for each instance of the real server.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to bind a server to multiple virtual servers:

```
SLB-Switch(config-slb-sfarm)# bindid 7
```

Related Commands

dfp
serverfarm
show module csm serverfarm

failaction purge

Use the **failaction purge** command in the SLB serverfarm configuration submode to set the behavior of connections to real servers that have failed. Use the **no** form of this command to disable the behavior of connections to real servers that have failed.

failaction purge

no failaction purge

Syntax Description

This command has no arguments or keywords.

Defaults

The default is **no failaction purge**.

Command Modes

SLB serverfarm configuration submode.

Usage Guidelines

With this command enabled, connections to a real server in the server farm are purged when the real server goes down. This feature is required for VPN load balancing.

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to set the behavior of connections to real servers that have failed:

```
SLB-Switch(config-slb-sfarm)# failaction purge
```

Related Commands

dfp
serverfarm
show module csm serverfarm

health

Use the **health** command in the SLB serverfarm configuration submode to set the retry attempts to real servers that have failed. Use the **no** form of this command to disable the retries or the time to wait for connections to real servers that have failed.

health retries *count* **failed** *seconds*

no health

Syntax Description

retries	Keyword to specify the number of tries to attempt to failed real servers.
count	Number of probes to wait before marking a server as failed; the range is from 0 to 65534.
failed	Keyword to specify the time to wait to attempt retries to the real servers.
seconds	Time in seconds before retrying a failed server; the range is from 0 to 65535.

Defaults

There are no default settings.

Command Modes

SLB serverfarm configuration submode.

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples

This example shows how to set the behavior of connections to real servers that have failed:

```
SLB-Switch(config-slb-sfarm)# health retries 20 failed 200
```

Related Commands

dfp
serverfarm
show module csm serverfarm

nat client

Use the **nat client** command in SLB serverfarm configuration submode to specify a set of client NAT pool addresses that should be used to perform the NAT function on clients connecting to this server farm. Use the **no** form of this command to remove the NAT pool from the configuration.

nat client *client-pool-name*

no nat client

Syntax Description

client-pool-name	Client pool name.

Defaults

This command has no default settings.

Command Modes

SLB serverfarm configuration submode.

Usage Guidelines

Use this command to enable client NAT. If client NAT is configured, the client address and port number in load-balanced packets are replaced with an IP address and port number from the specified client NAT pool. This client pool name must match the pool name entered from a previous **natpool** command.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify NAT on the client:

```
SLB-Switch(config-slb-sfarm)# nat client whishers
```

Related Commands

natpool
serverfarm
nat server
predictor
show module csm serverfarm

nat server

Use the **nat server** command in SLB serverfarm configuration submode to specify NAT to servers in this server farm. Use the **no** form of this command to disable server NAT.

nat server

no nat server

Syntax Description

This command has no arguments or keywords.

Defaults

Server NAT is enabled by default.

Command Modes

SLB server farm configuration submode.

Usage Guidelines

Use this command to enable server NAT. If server NAT is configured, the server address and port number in load-balanced packets are replaced with an IP address and port number of one of the real servers in the server farm.

Note The **nat server** command has no effect when **predictor forward** is configured, because no servers can be configured.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify NAT on the server:

```
SLB-Switch(config-slb-sfarm)# nat server
```

Related Commands

serverfarm
nat client
predictor
show module csm serverfarm

predictor

Use the **predictor** command in the SLB serverfarm configuration submode to specify the load-balancing algorithm for the server farm. Use the **no** form of this command to remove the load-balancing algorithm.

predictor {**roundrobin** | **leastconns** | **hash url** | **hash address** [**source** | **destination**] [*ip-netmask*] | **forward**}]

no predictor

Syntax Description

roundrobin	Keyword to select the next servers in the list of real servers.
leastconns	Keyword to select the server with the least number of connections.
hash url	Keyword to select the server using a hash value based on the URL.
hash address	Keyword to select the server using a hash value based on the source and destination IP addresses.
source	Keyword to select the server using a hash value based on the source IP address.
destination	Keyword to select the server using a hash value based on the destination IP address.
ip-netmask	(Optional) Bits in the IP address to use for the hash. If not specified, 255.255.255.255 is assumed.
forward	Keyword to tell the CSM to forward traffic in accordance with its internal routing tables.

Defaults

The default algorithm is round robin.

Command Modes

SLB serverfarm configuration submode.

Usage Guidelines

Use this command to define the load-balancing algorithm used in choosing a real server in the server farm. If you do not specify the **predictor** command, the default algorithm is **roundrobin**. Using the **no** form of this command changes the predictor algorithm to the default algorithm.

Note The **nat server** command has no effect when **predictor forward** is configured, because no servers can be configured.

The portion of the URL to hash is based on the expressions configured for the virtual server submode command **url-hash**.

No real servers are needed. The server farm is actually a route forwarding policy with no real servers associated with it.

5816
D.

Command History

Release	Modification
1.1(1)	This command was introduced.
2.1(1)	Changed the **ip-hash** to the **hash address source** keyword and added new keyword types of **hash address**, **hash address destination**, **hash url**, and **forward**. In addition, the **http-redirect** command is now hidden.

Examples

This example shows how to specify the load-balancing algorithm for the server farm:

```
SLB-Switch(config-module-csm)# serverfarm PUBLIC
SLB-Switch(config-slb-sfarm)# predictor leastconns
```

Related Commands

nat client
nat server
maxconns
minconns
serverfarm
show module csm serverfarm
serverfarm (SLB virtual server configuration submode)

probe

Use the **probe** command in the SLB serverfarm configuration submode to associate a probe with a server farm. Use the **no** form of this command to disable a specific probe.

probe *probe-name*

no probe *probe-name*

Syntax Description

probe-name	Probe name associated with the server farm.

Defaults

This command has no default settings.

Command Modes

SLB serverfarm configuration submode.

Usage Guidelines

Each server farm can be associated with multiple probes of the same or different protocols. Protocols supported by the CSM include HTTP, ICMP, TCP, FTP, SMTP, Telnet, and DNS.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to associate a probe with a server farm:

```
SLB-Switch(config-slb-sfarm)# probe general
```

Related Commands

probe (Module CSM configuration submode)
serverfarm
show module csm probe
show module csm serverfarm

retcode-map

Use the **retcode-map** command in the SLB serverfarm configuration submode to assign a return code map to a server farm. Use the **no** form of this command to disable a specific probe.

retcode-map *retcodemap_name*

no retcode-map

Syntax Description

retcodemap_name	Return code map name associated with the server farm.

Defaults

This command has no default settings.

Command Modes

SLB serverfarm configuration submode.

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples

This example shows how to associate a probe with a server farm:

```
SLB-Switch(config-slb-sfarm)# retcode-map return_stats
```

Related Commands

map retcode (Module CSM configuration submode)
serverfarm
show module csm serverfarm

show module csm arp

Use the **show module csm** *slot* **arp** command to display the CSM ARP cache.

show module csm *slot* **arp**

Syntax Description

slot	Slot where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb arp**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display the CSM ARP cache:

```
SLB-Switch# show module csm 4 arp

Internet Address  Physical Interface  VLAN      Type      Status
------------------------------------------------------------------
 10.10.3.100      00-01-64-F9-1A-02   0         VSERVER   local
 10.10.3.1        00-D0-02-58-B0-00   11        GATEWAY   up(0 misses)
 10.10.3.2        00-30-F2-71-6E-10   11/12     --SLB--   local
 10.10.3.10       00-D0-B7-82-38-97   12        REAL      up(0 misses)
 10.10.3.20       00-D0-B7-82-38-97   12        REAL      up(0 misses)
 10.10.3.30       00-D0-B7-82-38-97   12        REAL      up(0 misses)
 10.10.3.40       00-00-00-00-00-00   12        REAL      down(1 misses)
```

S912

show module csm conns

Use the **show module csm** *slot* **conns** command to display active connections.

show module csm *slot* **conns** [**vserver** *virtserver-name*] [**client** *ip-address*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
vserver	(Optional) Keyword to specify the connections associated with a particular virtual server.
virtserver-name	(Optional) Name of the virtual server to be monitored.
client	(Optional) Keyword to specify the connections associated with a particular client IP address.
ip-address	(Optional) IP address of the client to be monitored.
detail	(Optional) Keyword to specify detailed connection information.

Defaults

If no options are specified, the command displays output for all active connections.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb conns**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display active connection data:

```
SLB-Switch# show module csm 4 conns
prot vlan source                destination           state
----------------------------------------------------------------------
In  TCP  11   100.100.100.2:1754    10.10.3.100:80        ESTAB
Out TCP  12   100.100.100.2:1754    10.10.3.20:80         ESTAB

In  TCP  11   100.100.100.2:1755    10.10.3.100:80        ESTAB
Out TCP  12   100.100.100.2:1755    10.10.3.10:80         ESTAB

SLB-Switch# show module csm 4 conns detail

    prot vlan source                destination           state
----------------------------------------------------------------------
In  TCP  11   100.100.100.2:1754    10.10.3.100:80        ESTAB
Out TCP  12   100.100.100.2:1754    10.10.3.20:80         ESTAB
    vs = WEB_VIP, ftp = No, csrp = False

In  TCP  11   100.100.100.2:1755    10.10.3.100:80        ESTAB
Out TCP  12   100.100.100.2:1755    10.10.3.10:80         ESTAB
    vs = WEB_VIP, ftp = No, csrp = False
```

591
D

show module csm dfp

Use the **show module csm** *slot* **dfp** command to display DFP agent and manager information, such as passwords, timeouts, retry counts, and weights.

show module csm *slot* **dfp** [**agent** [**detail** | *ip-address port*] | **manager** [*ip_addr*] | **detail** | **weights**]

Syntax Description

slot	Slot where the CSM resides.
agent	(Optional) Keyword to specify information about a DFP agent.
detail	(Optional) Keyword to specify all data available.
ip_address	(Optional) Agent IP address.
port	(Optional) Agent port number.
manager	(Optional) Keyword to specify the agent and manager connection state and statistics, and the load and health metric sent to DFP manager.
ip_addr	(Optional) IP address of reported weights.
detail	(Optional) Keyword to specify all data available.
weights	(Optional) Keyword to specify information about weights assigned to real servers for load balancing.

Defaults

If no options are specified, the command displays summary information.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb dfp**.
2.1(1)	Added the virtual server weight display information to report to the DFP manager. This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows all available DFP data:

```
SLB-Switch# show module csm 4 dfp detail
```

This example shows information about weights:

```
SLB-Switch# show module csm 4 dfp weights
```

This example, with no options specified, shows summary information:

```
SLB-Switch# show module csm 4 dfp
```

show module csm ft

Use the **show module csm** *slot* **ft** command to display statistics and counters for the CSM fault-tolerant pair.

show module csm *slot* **ft [detail]**

Syntax Description

detail	(Optional) Keyword to display more detailed information.

Defaults

No values are displayed.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb ft**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display the statistics and counters for the CSM fault-tolerant pair:

```
SLB-Switch# show module csm 4 ft
FT group 2, vlan 30
 This box is active
 priority 10, heartbeat 1, failover 3, preemption is off
```

Related Commands

ft group

show module csm map

Use the **show module csm** *slot* **map** command to display information about URL maps.

show module csm *slot* **map [url | cookie | header | retcode] [name** *map-name***] [detail]**

Syntax Description

lot	Slot where the CSM resides.
ırl	(Optional) Keyword to specify only the URL map configuration.
ookie	(Optional) Keyword to specify only the cookie map configuration.
eader	(Optional) Keyword to specify only the header map configuration.
ɛtcode	(Optional) Keyword to specify only the return code map configuration.
ame	(Optional) Keyword to specify the named map.
ap-name	Map name to display.
ɛtail	(Optional) Keyword to specify all data available.

Defaults

is command has no default settings.

Command Modes

vileged EXEC.

Command History

ease	**Modification**
(1)	This command was introduced as **show ip slb map**.
(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only). The header option is added for displaying only header maps.
(1)	This command was changed to include the **retcode** option.

Examples

s example shows how to display URL maps associated with a Content Switching policy:

```
-Switch# show module csm 4 map url
 map UHASH_UMAP
OKIE map UHASH_CMAP1
OKIE map UHASH_CMAP2

show ip slb map detail
L map UHASH_UMAP rules:
aabb*

OKIE map UHASH_CMAP1 rules:
ame:foo  value:*asdgjasgdkjsdkgjsasdgsg*

OKIE map UHASH_CMAP2 rules:
ame:bar  value:*asdgjasgdkjsdkgjsasdgsg*
```

This example shows how to display return code maps:

```
SLB-Switch#show module csm 5 map retcode detail
 RETCODE map HTTPCODES rules:
  return codes:401 to 401  action:log     threshold:5  reset:120
  return codes:402 to 415  action:count   threshold:0  reset:0
  return codes:500 to 500  action:remove  threshold:3  reset:0
  return codes:503 to 503  action:remove  threshold:3  reset:0
```

Related Commands

map cookie
map header
map url

S906

show module csm memory

Use the **show module csm** *slot* **memory** command to display information about memory use.

show module csm *slot* **memory** [**vserver** *vserver-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
vserver	(Optional) Keyword to specify the virtual server configuration.
vserver-name	(Optional) Option to restrict output to the named virtual server.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb memory**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only). The **detail** keyword no longer has an effect and is hidden or deprecated.

Examples

This example shows how to display the memory usage of virtual servers:

```
SLB-Switch# show module csm 4 memory
slb vserver      total bytes   memory by type
---------------------------------------------------------------------------
WEB_VIP          0             0          0
FTP_VIP          0             0          0
Total(s):                    0          0
Out of Maximum:              261424     261344
```

Related Commands

parse-length (SLB virtual server configuration submode)

show module csm natpool

Use the **show module csm** *slot* **natpool** command to display NAT configurations.

show module csm *slot* **natpool** [**name** *pool-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Keyword to display a specific NAT pool.
pool-name	(Optional) NAT pool name string to display.
detail	(Optional) Keyword to list the interval ranges currently allocated in the client NAT pool.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb natpool**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display results of the default **show module csm** *slot* **natpool** command:

```
SLB-Switch# show module csm 4 natpool
nat client B  1.1(1).6  1.1(1).8  Netmask 255.255.255.0
        nat client A  1.1(1).1  1.1(1).5  Netmask 255.255.255.0
```

This example shows how to display results of the **show module csm** *slot* **natpool** command with the **detail** variable:

```
SLB-Switch# show module csm 4 natpool detail
nat client A  1.1(1).1  1.1(1).5  Netmask 255.255.255.0
     Start NAT         Last NAT          Count     ALLOC/FREE
     -------------------------------------------------------
     1.1(1).1:11001    1.1(1).1:16333    0005333    ALLOC
     1.1(1).1:16334    1.1(1).1:19000    0002667    ALLOC
     1.1(1).1:19001    1.1(1).5:65535    0264675    FREE
```

Related Commands

natpool

show module csm owner

Use the **show module csm** *slot* **owner** command to display the current connections count for the specified owner objects.

show module csm *slot* **owner** [**name** *owner-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
owner	Keyword to display a specific owner object.
name	(Optional) Keyword to display a specific owner object.
owner-name	(Optional) Owner object name string to display.
detail	(Optional) Keyword to list the virtual servers in an owner group with the vserver's state and current connections count.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Detailed information about an owner object lists the virtual servers in that group with each virtual server's state and current connections count.

The MAXCONNS state is displayed for a virtual server when the current connections counter is equal to the configured **maxconns** value. Counters for the number of connections dropped due to the virtual server being in this state are added. The **show module csm** *slot* **stats** and **show module csm** *slot* **vserver detail** command output displays these counters on a global and per-virtual server basis, respectively.

Examples

This example shows how to display results of the default **show module csm** *slot* **owner** command:

```
SLB-Switch# show module csm 4 owner
```

This example shows how to display results of the **show module csm** *slot* **owner** command with the **detail** variable:

```
SLB-Switch# show module csm 4 owner detail
```

Related Commands

owner
owner

show module csm policy

Use the **show module csm** *slot* **policy** command to display a policy configuration.

show module csm *slot* **policy** [**name** *policy-name*]

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Keyword to display a specific policy.
policy-name	(Optional) Policy name string to display.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb policy**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display a policy configuration:

```
SLB-Switch# show module csm 4 policy
policy:             PC1_UHASH_T1
sticky group:       20
serverfarm:         SF_UHASH_T1

policy:             PC1_UHASH_T2
sticky group:       30
serverfarm:         SF_UHASH_T2

policy:             PC1_UHASH_T3
url map:            UHASH_UMAP
serverfarm:         SF_UHASH_T3

policy:             PC1_UHASH_T4
cookie map:         UHASH_CMAP1
serverfarm:         SF_UHASH_T4

policy:             PC2_UHASH_T4
cookie map:         UHASH_CMAP2
serverfarm:         SF_UHASH_T4
SLB-Switch#
```

Related Commands

policy

5902
D

show module csm probe

Use the **show module csm** *slot* **probe** command to display HTTP or ping probe data.

show module csm *slot* **probe [http | icmp | telnet | tcp | ftp | smtp | dns] [name** *probe_name*] **[detail]**

Syntax Description

slot	Slot where the CSM resides.
http	(Optional) Keyword to display information about the HTTP configuration.
icmp	(Optional) Keyword to display information about the ICMP configuration.
telnet	(Optional) Keyword to display information about the Telnet configuration.
tcp	(Optional) Keyword to display information about the TCP configuration.
ftp	(Optional) Keyword to display information about the FTP configuration.
smtp	(Optional) Keyword to display information about the SMTP configuration.
dns	(Optional) Keyword to display information about the DNS configuration.
name	(Optional) Keyword to display information about the specific probe named.
probe_name	(Optional) Probe name to display.
detail	(Optional) Keyword to display detailed information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb probe**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display probe data:

```
SLB-Switch# show module csm 4 probe
probe              type      interval  retries  failed  open    receive
-----------------------------------------------------------------------
PB_ICMP1           icmp      60        1        5               10
PB_HTTP1           http      60        1        10       10     10
PB_TCP1            tcp       60        1        10       10     10
```

```
PB_FTP1          ftp       60        1         10        10       10
PB_TELNET1       telnet    60        1         10        10       10
PB_SMTP1         smtp      60        1         10        10       10
```

Related Commands **probe**

5900 D

show module csm probe script

Use the **show module csm** *slot* **probe script [name** *probe -name***] [detail]** command to display probe script data.

show module csm *slot* **probe script [name** *probe -name***] [detail]**

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Keyword to display information about the specific probe named.
probe_name	(Optional) Probe name to display.
detail	(Optional) Keyword to display detailed information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to display probe data:

```
SLB-Switch# show module csm 4 probe script detail
```

Related Commands

probe

probe script, page A-62

show module csm real

Use the **show module csm** *slot* **real** command to display information about real servers.

show module csm *slot* **real** [**sfarm** *sfarm-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
sfarm	(Optional) Keyword to displays real servers for only a single serverfarm.
sfarm-name	(Optional) Name of the server farm to restrict output.
detail	(Optional) Keyword to display detailed information.

Defaults

If no options are specified, the command displays information about all real servers.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb real**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows Cisco IOS SLB real server data:

```
SLB-Switch# show module csm 4 real
real                  server farm      weight  state          conns
-------------------------------------------------------------------
10.10.3.10            FARM1            20      OPERATIONAL    0
10.10.3.20            FARM1            16      OUTOFSERVICE   0
10.10.3.30            FARM1            10      OPERATIONAL    0
10.10.3.40            FARM1            10      FAILED         0
SLB-Switch# show mod csm 5 real detail
10.1.0.102, FARM1, state = OPERATIONAL
  Inband health:remaining retries = 3
  conns = 0, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  total conns established = 0, total conn failures = 0
10.1.0.101, FARM1, state = OPERATIONAL
  Inband health:remaining retries = 3
  conns = 0, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 0
  total conns established = 0, total conn failures = 0
10.1.0.101, FARM2, state = OPERATIONAL
  conns = 2, maxconns = 4294967295, minconns = 0
  weight = 8, weight(admin) = 8, metric = 0, remainder = 2
  total conns established = 7, total conn failures = 0
```

5898
D

Table A-1 describes the fields in the display.

Table A-1 show module csm real Command Field Information

Field	Description
real	Information about each real server is displayed on a separate line.
server farm	Name of the server farm associated to the real server.
weight	Weight assigned to the real server. The weight identifies the capacity of the real server compared to other real servers in the server farm.
state	Current state of the real server: • OUTOFSERVICE—Removed from the load-balancing predictor lists. • FAILED—Removed from use by the predictor algorithms that start the retry timer. • OPERATIONAL—Functioning properly. • MAXCONNS • DFP_THROTTLED • PROBE_FAILED • PROBE_TESTING • TESTING—Queued for assignment. • READY_TO_TEST—Device functioning and ready to test.
conns	Number of connections.

Related Commands **real** (SLB serverfarm configuration submode)

show module csm real retcode

Use the **show module csm** *slot* **real retcode** command to display information about the return code configuration.

show module csm *slot* **real retcode [sfarm** *sfarm-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
sfarm	(Optional) Keyword to displays real servers for only a single server farm.
sfarm-name	(Optional) Name of the server farm to restrict output.
detail	(Optional) Keyword to display detailed information.

Defaults

If no options are specified, the command displays information about all real servers.

Command Modes

Privileged EXEC.

Command History

Release	Modification
2.2.1	This command was introduced.

Examples

This example shows Cisco IOS SLB real server return code data:

```
SLB-Switch# show module csm 5 real retcode
10.1.0.101, FARM2, state = OPERATIONAL
  retcode-map = HTTPCODES
  retcode  action   count      reset-seconds  reset-count
  ------------------------------------------------------
  401      log      3          0              1
  404      count    62         0              0
  500      remove   1          0              0
```

Related Commands

real (SLB serverfarm configuration submode)

5896
9

show module csm script

Use the **show module csm** *slot* **script** command to display the contents of all loaded scripts.

show module csm *slot* **script** [**name** *full_file_URL*] [**code**]

Syntax Description

slot	Slot where the CSM resides.
script	Keyword to display script information.
name	(Optional) Keyword to display information about a particular script.
full_file_URL	(Optional) Name of the script.
code	(Optional) Keyword to display the contents of the script.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to display script file contents:

```
SLB-Switch# show module csm slot script [name script-name] [code]
```

Related Commands

script file

show module csm script task

Use the **show module csm** *slot* **script task** command to display all loaded scripts.

show module csm slot **script task [index** *script-index***] [detail]**

Syntax Description

slot	Slot where the CSM resides.
script task	Keyword to display script task information.
index	(Optional) Keyword to display information about a particular script.
script-index	(Optional)
detail	(Optional) Keyword to display the contents of the script.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to display A running script:

```
SLB-Switch# show module csm slot script
```

Related Commands

script file
script task
show module csm script

show module csm serverfarm

Use the **show module csm** *slot* **serverfarm** command to display information about a server farm.

show module csm *slot* **serverfarms** [**name** *serverfarm-name*] [**detail**]

Syntax Description

slot	Slot where the CSM resides.
name	(Optional) Keyword to display information about a particular server farm.
serverfarm-name	(Optional) Name of the server farm.
detail	(Optional) Keyword to display detailed server farm information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb serverfarm**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display server farm data:

```
SLB-Switch# show module csm 4 serverfarm
server farm      predictor    nat   reals   redirect  bind id
------------------------------------------------------------
FARM1            RoundRobin   S     4       0         0
VIDEO_FARM       RoundRobin   S     5       0         0
AUDIO_FARM       RoundRobin   S     2       0         0
FTP              RoundRobin   S     3       0         0
```

Table A-2 describes the fields in the display.

Table A-2 show module csm serverfarms Command Field Information

Field	Description
server farm	Name of the server farm about which information is being displayed. Information about each server farm is displayed on a separate line.
predictor	Type of load-balancing algorithm) used by the server farm.
nat	Shows whether server and client NAT is enabled.
reals	Number of real servers configured in the server farm.

Table A-2 show module csm serverfarms Command Field Information (continued)

Field	Description
redirect	Number of redirect virtual servers configured in the server farm.
bind id	Bind ID configured on the server farm.

This example shows how to display only the details for one server farm:

```
SLB-Switch# show mod csm 5 serverfarm detail
FARM1, predictor = RoundRobin, nat = SERVER, CLIENT(CLNAT1)
 virtuals inservice:4, reals = 2, bind id = 0, fail action = none
 inband health config:retries = 3, failed interval = 200
 retcode map = <none>
 Real servers:
 10.1.0.102, weight = 8, OPERATIONAL, conns = 0
 10.1.0.101, weight = 8, OPERATIONAL, conns = 0
 Total connections = 0

FARM2, predictor = RoundRobin, nat = SERVER, CLIENT(CLNAT1)
 virtuals inservice:2, reals = 1, bind id = 0, fail action = none
 inband health config:<none>
 retcode map = HTTPCODES
 Real servers:
 10.1.0.101, weight = 8, OPERATIONAL, conns = 2
 Total connections = 2
```

Related Commands **serverfarm**

show module csm static

Use the **show module csm** *slot* **static** command to display information about server NAT configurations.

show module csm *slot* **static** [**drop** | **nat** {*ip-address* | **virtual**}]

Syntax Description

slot	Slot where the CSM resides.
drop	(Optional) Keyword to display information about real servers configured to drop connections.
nat	(Optional) Keyword to display information about real servers configured to NAT.
ip-address	(Optional) IP address to which to NAT.
virtual	(Optional) Keyword to display information about real servers configured to NAT virtual server IP addresses.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb static**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display static data:

```
SLB-Switch# show module csm 4 static nat
```

Related Commands

static
real (SLB static NAT configuration submode)

show module csm static server

Use the **show module csm** *slot* **static server** command to display information about actual servers that are having NAT performed.

show module csm *slot* **static server** [*ip-address*] [**drop** | **nat** {*ip-address* | **virtual**} | **pass-through**]

Syntax Description

slot	Slot where the CSM resides.
ip-address	(Optional) Option to limit output to a specified server address.
drop	(Optional) Keyword to display information about real servers configured to drop connections.
nat	(Optional) Keyword to display information about real servers configured to NAT.
ip-address	(Optional) IP address to NAT.
virtual	(Optional) Keyword to display information about servers configured to NAT virtual server addresses.
pass-through	(Optional) Keyword to display detailed information about real servers with no NAT configured.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb static server**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display static server data:

```
SLB-Switch# show module csm 4 static server

Server           NAT Type
---------------------------------------------
10.10.3.10       NAT to 100.100.100.100
10.10.3.20       No NAT
10.10.3.30       NAT to 100.100.100.100
10.10.3.40       No NAT
Cat6k-1#
```

Related Commands

static
real (SLB static NAT configuration submode)

5890

show module csm stats

Use the **show module csm** *slot* **stats** command to display SLB statistics.

show module csm *slot* **stats**

Syntax Description

slot	Slot where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb stats**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display SLB statistics:

```
SLB-Switch# show module csm 4 stats
Connections Created:        180
Connections Destroyed:      180
Connections Current:        0
Connections Timed-Out:      0
Connections Failed:         0
Server initiated Connections:
      Created:0, Current:0, Failed:0
L4 Load-Balanced Decisions:180
L4 Rejected Connections:    0
L7 Load-Balanced Decisions:0
L7 Rejected Connections:
      Total:0, Parser:0,
      Reached max parse len:0, Cookie out of mem:0,
      Cfg version mismatch:0, Bad SSL2 format:0
L4/L7 Rejected Connections:
      No policy:0, No policy match 0,
      No real:0, ACL denied 0,
      Server initiated:0
Checksum Failures: IP:0, TCP:0
Redirect Connections:0,  Redirect Dropped:0
FTP Connections:            0
MAC Frames:
      Tx:Unicast:1506, Multicast:0, Broadcast:50898,
          Underflow Errors:0
      Rx:Unicast:2385, Multicast:6148349, Broadcast:53916,
          Overflow Errors:0, CRC Errors:0
```

Table A-3 describes the fields in the display.

Table A-3 show module csm stats Command Field Information

Field	Description
Connections Created	Number of connections that have been created since the last time counters were cleared.
Connections Destroyed	Number of connections that have been destroyed since the last time counters were cleared.

5788
0

show module csm status

Use the **show module csm** *slot* **status** command to display if the CSM is online. If the CSM is online, this command shows the CSM chassis slot location and indicates if the configuration download is complete.

show module csm *slot* **status**

Syntax Description

slot	Slot where the CSM resides.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb status**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display CSM status:

```
SLB-Switch# show module csm 4 status
SLB Module is online in slot 4.
Configuration Download state:COMPLETE, SUCCESS
```

show module csm sticky

Use the **show module csm** *slot* **sticky** command to display the sticky database.

show module csm *slot* **sticky** [**groups** | **client** *ip_address*]

Syntax Description

slot	Slot where the CSM resides.
groups	(Optional) Keyword to display all of the sticky group configurations.
client	(Optional) Keyword to display the sticky database entries associated with a particular client IP address.
ip_address	(Optional) IP address of the client.

Defaults

If no options are specified, the command displays information about all clients.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb sticky**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only.

Usage Guidelines

This command only displays the database of clients using IP stickiness; it does not show cookie or SSL.

Examples

This example shows how to display the sticky database:

```
SLB-Switch# show module csm 4 sticky groups
Group  Timeout  Type
---------------------------------------------------------------
20     100      netmask 255.255.255.255
30     100      cookie foo
```

Related Commands

sticky
sticky (SLB virtual server configuration submode)

3886

show module csm tech-script

Use the **show module csm** *slot* **tech-script** command to display the status of a script.

show module csm *slot* **tech-script**

Syntax Description

slot	Slot where the CSM resides.

Defaults

If no options are specified, the command displays all information.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to display the technical support information for the CSM:

```
SLB-Switch# show module csm 4 tech-script
```

show module csm tech-support

Use the **show module csm** *slot* **tech-support** command to display technical support information for the CSM.

show module csm *slot* **tech-support [all | processor** *num* **| redirect | slowpath | probe | fpga | core-dump]**

Syntax Description

slot	Slot where the CSM resides.
all	(Optional) Keyword to display all of the available statistics.
processor	(Optional) Keyword to display the IXP statistics for the IXP identified by *num*.
num	(Optional) IXP number.
redirect	(Optional) Keyword to display all of the HTTP redirect statistics
slowpath	(Optional) Keyword to display all of the slowpath statistics.
probe	(Optional) Keyword to display all of the probe statistics.
fpga	(Optional) Keyword to display all of the FPGA statistics.
core_dump	(Optional) Keyword to display all of the most recent statistics for the process (IXP or Power PC) that experienced a core dump.

Defaults

If no options are specified, the command displays all information.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb tech-support.**
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display the technical support information for the CSM:

```
SLB-Switch# show module csm 4 tech-support ?
  all         All tech output
  core-dump   Most recent core dump
  fpga        FPGA info output
  ft          Fault Tolerance info output
  probe       Probe info output
  processor   Processor info output
  redirect    HTTP redirect info output
  slowpath    Slowpath info output

SLB-Switch# show module csm 4 tech-support processor 2
---------------------------------------------------------------
----------------------- TCP Statistics ------------------------
---------------------------------------------------------------
```

```
     Aborted rx                                 3350436013  66840864
     New sessions rx                            180         0
     Total Packets rx                           16940       0
     Total Packets tx                           0           0
     Packets Passthrough                        697         0
     Packets Dropped                            0           0
     Persistent OOO Packets Dropped             0           0
     Persistent Fastpath Tx                     0           0
     Total Persistent Requests                  0           0
     Persistent Same Real                       0           0
     Persistent New Real                        0           0

     Data Packets rx                            877         0
     L4 Data Packets rx                         877         0
     L7 Data Packets rx                         0           0
     Slowpath Packets rx                        7851        0
     Relinquish Requests rx                     8031        0

     TCP xsum failures                          0           0

     Session Mismatch                           0           0
     Session Reused while valid                 0           0
     Unexpected Opcode rx                       0           0
     Unsupported Proto                          0           0
     Session Queue Overflow                     0           0
     Control->Term Queue Overflow               0           0
     t_fifo Overflow                            0           0

     L7 Analysis Request Sent                   0           0
     L7 Successful LB decisions                 0           0
     L7 Need More Data decisions                0           0
     L7 Unsuccessful LB decisons                0           0
     L4 Analysis Request Sent                   180         0
     L4 Successful LB decisions                 180         0
     L4 Unsuccessful LB decisons                0           0

Transmit:
       SYN                                      0           0
       SYN/ACK                                  0           0
       ACK                                      0           0
       RST/ACK                                  0           0
       data                                     0           0
     Retransmissions:                          0           0
Receive:
       SYN                                      180         0
       SYN/ACK                                  0           0
       ACK                                      340         0
       FIN                                      0           0
       FIN/ACK                                  340         0
       RST                                      17          0
       RST/ACK                                  0           0
       data                                     0           0

Session Redundancy Standby:
     Rx Fake SYN                                0           0
     Rx Repeat Fake SYN                         0           0
     Rx Fake Reset                              0           0
     Fake SYN Sent to NAT                       0           0
     Tx Port Sync                               0           0
     Encap Not Found                            0           0
     Fake SYN, TCP State Invalid                0           0

Session Redundancy Active:
     L4 Requests Sent                           0           0
```

```
L7 Requests Sent                            0           0
Persistent Requests Sent                    0           0
Rx Fake SYN                                 0           0
Fake SYN Sent to NAT                        0           0

Session's torn down                         180         0
Rx Close session                            1           0
Slowpath(low  pri) buffer allocs            7843        0
Slowpath(high pri) buffer allocs            8           0
Small buffer allocs                         180         0
Medium buffer allocs                        0           0
Large buffer allocs                         0           0
Session table allocs                        180         0

Slowpath(low  pri) buffer alloc failures    0           0
Slowpath(high pri) buffer alloc failures    0           0
Small buffer allocs failures                0           0
Medium buffer allocs failures               0           0
Large buffer allocs failures                0           0
Session table allocs failures               0           0

Outstanding slowpath(low  pri) buffers      0           0
Outstanding slowpath(high pri) buffers      0           0
Outstanding small buffers                   0           0
Outstanding medium buffers                  0           0
Outstanding large buffers                   0           0
Outstanding sessions                        0           0
```

5882
D

show module csm vlan

Use the **show module csm** *slot* **vlan** command to display the list of VLANs.

show module csm *slot* **vlan [client | server | ft] [id** *vlan-id*] **[detail]**

Syntax Description

slot	Slot where the CSM resides.
client	(Optional) Keyword to display only the client VLAN configuration.
server	(Optional) Keyword to display only the server VLAN configuration.
ft	(Optional) Keyword to display only the fault-tolerant configuration.
id	(Optional) Keyword to display the VLAN.
vlan-id	(Optional) Keyword to display the specified VLAN.
detail	(Optional) Keyword to display the map configuration details.

Defaults

If no options are specified, the command displays information about all VLANs.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb vlan**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display the VLAN configurations:

```
SLB-Switch# show module csm 4 vlan

vlan   IP address       IP mask          type
---------------------------------------------------
11     10.10.4.2        255.255.255.0    CLIENT
12     10.10.3.1        255.255.255.0    SERVER
30     0.0.0.0          0.0.0.0          FT
SLB-Switch#
SLB-Switch#
SLB-Switch# sh mod csm 4 vlan detail
vlan   IP address       IP mask          type
---------------------------------------------------
11     10.10.4.2        255.255.255.0    CLIENT
  GATEWAYS
  10.10.4.1
12     10.10.3.1        255.255.255.0    SERVER
30     0.0.0.0          0.0.0.0          FT
```

Related Commands

vlan - Module CSM configuration submode.

show module csm vserver redirect

Use the **show module csm** *slot* **vserver redirect** command to display the list of virtual servers.

show module csm *slot* **vserver redirect**

Syntax Description

slot	Slot where the CSM resides.

Defaults

If no options are specified, the command displays information about all clients.

Command Modes

Privileged EXEC.

Command History

Release	Modification
1.1(1)	This command was introduced as **show ip slb vserver redirect**.
2.1(1)	This command was changed to **show module csm** *slot* (for **ip slb mode rp** only).

Examples

This example shows how to display the CSM virtual servers:

```
SLB-Switch# show module csm 4 vserver

slb vserver      prot  virtual                   vlan  state         conns
-------------------------------------------------------------------------------
FTP_VIP          TCP   10.10.3.100/32:21         ALL   OUTOFSERVICE  0
WEB_VIP          TCP   10.10.4.100/32:80         ALL   OPERATIONAL   0
SLB-Switch#
SLB-Switch#
SLB-Switch# sh mod csm 4 vserver detail
FTP_VIP, state = OUTOFSERVICE, v_index = 3
  virtual = 10.10.3.100/32:21, TCP, service = NONE, advertise = FALSE
  idle = 3600, replicate csrp = none, vlan = ALL
  max parse len = 600, persist rebalance = TRUE
  conns = 0, total conns = 0
  Policy            Tot Conn     Client pkts  Server pkts
  -------------------------------------------------------
  (default)         0            0            0

WEB_VIP, state = OPERATIONAL, v_index = 4
  virtual = 10.10.4.100/32:80, TCP, service = NONE, advertise = FALSE
  idle = 3600, replicate csrp = none, vlan = ALL
  max parse len = 600, persist rebalance = TRUE
  conns = 0, total conns = 140
  Default policy:
    server farm = FARM1
    sticky:timer = 0, subnet = 0.0.0.0, group id = 0
  Policy            Tot Conn     Client pkts  Server pkts
  -------------------------------------------------------
  (default)         140          672          404
```

show module csm xml stats

Use the **show module csm xml stats** command to display a list of XML statistics.

show module csm xml stats

Defaults

If no options are specified, the command displays information about all clients.

Command Modes

Privileged EXEC.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to display the CSM XML statistics:

```
SLB-Switch# show module csm 4 xml stats
XML config:inservice, port = 80, vlan = <all>, client list = <none>
   connection stats:
     current = 0, total = 5
     failed = 2, security failed = 2
   requests:total = 5, failed = 2
```

S878
D

snmp enable traps slb ft

Use the **snmp enable traps slb ft** command to enable or disable fault-tolerant traps. Use the **no** form of this command to disable fault-tolerant traps.

snmp enable traps slb ft

no snmp enable traps slb ft

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

A fault-tolerant trap allows the CSM e to send an SNMP trap when the CSM transitions from standby to active after detecting a failure in its fault tolerant peer.

Examples

This example shows how to enable fault tolerant traps:

```
SLB-Switch(config-module-csm)# snmp enable traps slb ft
```

static

Use the **static** command to configure the server NAT behavior and enter the NAT configuration submode. This command configures the CSM to support connections initiated by real servers. Both client NAT and server NAT can exist in the same configuration. Use the **no** form of this command to remove NAT from the CSM configuration.

static {**drop** | **nat** {**virtual** | *ip-address*}}

no static {**drop** | **nat** {**virtual** | *ip-address*}}

Syntax Description

drop	Keyword to drop connections from servers specified in static submode.
virtual	Keyword specifying that the configuration is for NAT.
nat	Keyword to use the server's Virtual IP (VIP) to NAT its source IP address.
ip-address	IP address to be used for NAT.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to configure the CSM to support connections initiated by the real servers:

```
SLB-Switch(config-module-csm)# static nat virtual
```

Related Commands

show module csm static

58x0 9

real

Use the **real** command in SLB static NAT configuration submode to specify the address for a real server or the subnet mask for multiple real servers performing server NAT. Use the **no** form of this command to remove the address of a real server or the subnet mask of multiple real servers so they are no longer performing NAT.

real *real-ip-address* [*real-netmask*]

no real *real-ip-address* [*real-netmask*]

Syntax Description

real-ip-address	Real server IP address performing NAT.
real-netmask	(Optional) Range of real servers performing NAT. If not specified, the default is 255.255.255.255 (a single real server).

Defaults

This command has no default settings.

Command Modes

SLB static NAT configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify the address for a real server:

```
SLB-Switch(config-slb-static)# real 10.0.0.0 255.0.0.0
```

Related Commands

static
show module csm static

sticky

Use the **sticky** command to ensure that connections from the same client that match the same SLB policy use the same real server on subsequent connections. Use the **no** form of this command to remove a sticky group.

sticky *sticky-group-id* {**netmask** *netmask* | **cookie** *name* | **ssl**} [**timeout** *sticky-time*]

no sticky s*ticky-group-id*

Syntax Description

sticky-group-id	ID to identify the sticky group instance; the range is from 1 to 255.
netmask	Keyword to specify the network mask for IP stickiness.
netmask	Network mask number.
cookie	Keyword to specify cookie stickiness.
name	Name of the cookie attached to the *sticky-group-id*.
ssl	Keyword to specify SSL stickiness.
timeout	(Optional) Keyword to specify the sticky duration.
sticky-time	(Optional) Sticky timer duration in minutes; the range is from 0 to 65535.

Defaults

The sticky time default value is 1440 minutes (24 hours).

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.
2.1(1)	Changed the default timeout from 0 to 1440.

Usage Guidelines

Specifying a netmask permits sticky connections based on the masked client IP address.

Use the sticky time option to ensure that connections from the same client that match the same SLB policy use the same real server. If you specify a nonzero value, the last real server that was used for a connection from a client is remembered for *sticky-time* minutes after the end of the client's latest connection. New connections from the client to the virtual server initiated before the sticky time expires and that match SLB policy are balanced to the same real server that was used for the previous connection. A sticky time of 0 means sticky connections are not tracked.

Examples

This example shows how to create an IP sticky group:

```
SLB-Switch(config-module-csm)# sticky 5 netmask 255.255.255.255 timeout 20
```

vlan

Use the **vlan** command to create a client or server VLAN and assign it a VLAN ID and enter the VLAN submode. Use the **no** form of this command to remove the VLAN from the configuration.

vlan *vlan-id* {**client** | **server**}

no vlan *vlan-id*

Syntax Description

vlan-id	Number of the VLAN; the range is from 2 to 4095.
client	Keyword to specify a client-side VLAN.
server	Keyword to specify a server-side VLAN.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Usage Guidelines

A database entry should exist for the given VLAN ID.

Command History

Release	Modification
1.1(1)	This command was introduced.
2.1(1)	VLAN type fault-tolerance is deprecated and hidden.

Examples

This example shows how to create a server VLAN and assign it a VLAN ID:

```
SLB-Switch(config-module-csm)# vlan 2 server
```

Related Commands

vlan (SLB vserver submode)
show module csm vlan

15872 D

alias

Use the **alias** command in the SLB VLAN configuration submode to assign multiple IP addresses to the CSM. Use the **no** form of this command to remove an alias IP addresses from the configuration.

alias *ip-address netmask*

no alias *ip-address netmask*

Syntax Description

ip-address	Alias IP address; a maximum of 255 addresses are allowed per VLAN.
netmask	Network mask.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode.

Usage Guidelines

This command allows you to place the CSM on a different IP network than real servers without using a router.

Command History

Release	Modification
1.1(1)	This command was introduced for server VLANs.
2.1(1)	This command is now available for both client and server VLANs.

Examples

This example shows how to assign multiple IP addresses to the CSM:

```
SLB-Switch(config-slb-vlan-server)# alias 130.21.34.56 255.255.255.0
SLB-Switch(config-slb-vlan-server)# alias 130.22.35.57 255.255.255.0
SLB-Switch(config-slb-vlan-server)# alias 130.23.36.58 255.255.255.0
SLB-Switch(config-slb-vlan-server)# alias 130.24.37.59 255.255.255.0
SLB-Switch(config-slb-vlan-server)# alias 130.25.38.60 255.255.255.0
```

Related Commands

vlan
show module csm vlan

5871
D.

gateway

Use the **gateway** command in the SLB VLAN configuration mode to configure a gateway IP address. Use the **no** form of this command to remove the gateway from the configuration.

gateway *ip-address*

no gateway *ip-address*

Syntax Description

ip-address	IP address of the client-side gateway.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode.

Usage Guidelines

You can configure up to seven gateways per VLAN with a total of up to 255 gateways for the entire system. A gateway must be in the same network as specified in the **ip address** SLB VLAN command.

Command History

Release	Modification
1.1(1)	This command was introduced for client VLANs.
2.1(1)	This command is now available for both client and server VLANs.

Examples

This example shows how to configure a client-side gateway IP address:

```
SLB-Switch(config-slb-vlan-client)# gateway 130.21.34.56
```

Related Commands

ip address (SLB VLAN configuration submode)
vlan
show module csm vlan

ip address

Use the **ip address** command in the SLB VLAN configuration submode to assign an IP address to the CSM that is used for probes and ARP requests on a VLAN. Use the **no** form of this command to remove the CSM IP address and disable probes and ARP requests from the configuration.

ip address *ip-address netmask*

no ip address

Syntax Description

ip-address	IP address for the CSM; only one management IP address is allowed per VLAN.
netmask	Network mask.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode.

Usage Guidelines

This command is applicable for both server and client VLANs. Up to 255 unique VLAN IP addresses are allowed per module.

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2.1	Increases maximum number of unique VLAN IP addresses per system form 32 to 255.

Examples

This example shows how to assign an IP address to the CSM:

```
SLB-Switch(config-slb-vlan-client)# ip address 130.21.34.56 255.255.255.0
```

Related Commands

vlan
show module csm vlan

route

Use the **route** command in the SLB VLAN configuration submode to configure networks that are one Layer 3 hop away from the CSM. Use the **no** form of this command to remove the subnet or gateway IP address from the configuration.

route *ip-address netmask* **gateway** *gw-ip-address*

no route *ip-address netmask* **gateway** *gw-ip-address*

Syntax Description

ip-address	Subnet IP address.
netmask	Network mask.
gateway	Keyword to specify that the gateway is configured.
gw-ip-address	Gateway IP address.

Defaults

This command has no default settings.

Command Modes

SLB VLAN configuration submode.

Usage Guidelines

You specify the Layer 3 network's subnet address and the gateway IP address to reach the next-hop router. The gateway address must be in the same network as specified in the **ip address** SLB VLAN command.

Command History

Release	Modification
1.1(1)	This command was introduced for server VLANs.
2.1(1)	This command is now available for both client and server VLANs.

Examples

This example shows how to configure a network to the CSM:

```
SLB-Switch(config-slb-vlan-server)# route 130.21.34.56 255.255.255.0 gateway 120.22.36.40
```

Related Commands

ip address (SLB VLAN configuration submode)
vlan
show module csm vlan

5868 D

vserver

Use the **vserver** command to identify a virtual server and enter the virtual server configuration submode. Use the **no** form of this command to remove a virtual server from the configuration.

vserver *virtserver-name*

no vserver *virtserver-name*

Syntax Description

virtserver-name	Character string used to identify the virtual server; the character string is limited to 15 characters.

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to identify a virtual server named PUBLIC_HTTP and change the CLI to virtual server configuration mode:

```
SLB-Switch(config-module-csm)#   vserver PUBLIC_HTTP
```

Related Commands

redirect-vserver (SLB serverfarm submode)
show module csm vserver redirect

advertise

Use the **advertise** command in the SLB t virtual server configuration mode to allow the CSM to advertise the IP address of the virtual server as host-route. Use the **no** form of this command to stop advertising the host-route for this virtual server.

advertise [active]

no advertise

Syntax Description

active	(Optional) Keyword to allow the CSM to advertise the IP address of the virtual server as host-route.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

Without the active option, the CSM always advertises the virtual server IP address whether or not there is any active real server attached to this virtual server.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to restrict a client from using the virtual server:

```
SLB-Switch(config-slb-redirect-vs)# advertise 10.5.2.1 exclude
```

Related Commands

redirect-vserver
show module csm vserver redirect

5866
D

client

Use the **client** command in the SLB virtual server configuration mode to restrict which clients are allowed to use the virtual server. Use the **no** form of this command to remove the client definition from the configuration.

client *ip-address* [*network-mask*] [**exclude**]

no client *ip-address* [*network-mask*]

Syntax Description

ip-address	Client's IP address.
network-mask	(Optional) Client's IP mask.
exclude	(Optional) Keyword to specify that the IP address is disallowed.

Defaults

The default for network mask is 255.255.255.255 if the network mask is not specified.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

The network mask is applied to the source IP address of incoming connections and the result must match the IP address before the client is allowed to use the virtual server. If exclude is not specified, the IP address and network mask combination is allowed.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to restrict a client from using the virtual server:

```
SLB-Switch(config-slb-vserver)# client 10.5.2.1 exclude
```

Related Commands

client-group (SLB policy submode)
ip access-list standard
vserver
show module csm vserver redirect

5865
D.

idle

Use the **idle** command in the SLB virtual server configuration submode to control the amount of time the CSM maintains connection information in the absence of packet activity. Use the **no** form of this command to change the idle timer to its default value.

idle *duration*

no idle

Syntax Description

duration	Idle connection timer duration in seconds; the range is from 4 to 65535.

Defaults

The default is 3600.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

If you do not specify a duration value, the default value is applied.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to specify an idle timer duration of 4000:

```
SLB-Switch(config-slb-vserver)# idle 4000
```

Related Commands

vserver
show module csm vserver redirect

5884

D.

inservice

Use the **inservice** command in the SLB virtual server configuration submode to enable the virtual server for load balancing. Use the **no** form of this command to remove the virtual server from service.

inservice

no inservice

Syntax Description

This command has no keywords or arguments.

Defaults

The default is **no inservice**.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to enable a virtual server for load balancing:

```
SLB-Switch(config-slb-vserver)# inservice
```

Related Commands

vserver
show module csm vserver redirect

5863
D

owner

Use the **owner** command in the SLB virtual server submode to define an owner that may access the virtual server. Use the **no** form of this command to remove the owner.

owner *owner-name* ***maxconns*** *number*

no maxconns

Syntax Description

owner-name	Name of the owner object.
maxconns	Keyword to set the maximum number of connections for this owner.
number	Maximum number of connections.

Defaults

This command has no default settings.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to specify an owner for virtual server access:

```
SLB-Switch(config-slb-vserver)# owner madrigal maxconns 1000
```

Related Commands

vserver

parse-length

Use the **parse-length** command in the SLB virtual server configuration submode to set the maximum number of bytes to parse for URLs and cookies. Use the **no** form of this command to restore the default.

parse-length *bytes*

no parse-length

Syntax Description

bytes	Number of bytes; the range is from 1 to 4000.

Defaults

The default is 600.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to set the number of bytes to parse for URLs and cookies:

```
SLB-Switch(config-slb-vserver)# parse-length 1000
```

Related Commands

vserver
show module csm vserver redirect

pending

Use the **pending** command in the SLB virtual server configuration submode to set the pending connection timeout. Use the **no** form of this command to restore the default.

pending *timeout*

no pending

Syntax Description

timeout	Seconds to wait before a connection is considered unreachable. Range is from 1 to 65535.

Defaults

The default pending timeout is 30 seconds.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

This command is used to prevent denial of service (DOS) attacks. The pending connection timeout sets the response time for terminating connections if a switch becomes flooded with traffic. The pending connections are configurable on a per virtual server basis.

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples

This example shows how to set the number to wait for a connection to be made to the server:

```
SLB-Switch(config-slb-vserver)# pending 300
```

Related Commands

vserver
show module csm vserver redirect

5860
D

persistent rebalance

Use the **persistent rebalance** command in the SLB virtual server configuration submode to enable or disable HTTP 1.1 persistence for connections in the virtual server. Use the **no** form of this command to disable persistence.

persistent rebalance

no persistent rebalance

Syntax Description

This command has no keywords or arguments.

Defaults

The default is **persistent rebalance**.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to enable the HTTP 1.1 persistence:

```
SLB-Switch(config-slb-vserver)# persistent rebalance
```

Related Commands

vserver
show module csm vserver redirect

replicate csrp

Use the **replicate csrp** command in the SLB virtual server configuration submode to enable connection redundancy. Use the **no** form of this command to disable connection redundancy.

replicate csrp {**sticky** | **connection**}

no replicate csrp {**sticky** | **connection**}

Syntax Description

sticky	Replicate the sticky database to the backup CSM.
connection	Replicate connections to the backup CSM.

Defaults

The default is disabled.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

Sticky and connection replication can be enabled or disabled separately. For replication to occur, you must enable SLB fault tolerance with the **ft group** command.

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to enable connection redundancy:

```
SLB-Switch(config-slb-vserver)# replicate csrp connection
```

Related Commands

ft group
vserver
show module csm vserver redirect

5858

serverfarm

Use the **serverfarm** command in SLB virtual server configuration submode to associate a server farm with a virtual server. Use the **no** form of this command to remove a server farm association from the virtual server.

serverfarm *primary-serverfarm* [**backup** *sorry-serverfarm* [**sticky**]]

no serverfarm

Syntax Description

primary-sf	Character string used to identify the server farm.
backup	(Optional) Keyword set the name of a backup serverfarm.
sorry-sf	(Optional) Backup serverfarm name.
sticky	(Optional) Keyword to associate the backup serverfarm with a virtual server.

Defaults

This command has no default settings.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

The server farm name must match the server farm name specified in a previous module CSM submode **serverfarm** command.

The backup serverfarm can be associated with a policy. A primary serverfarm must be associated with that policy to allow the backup serverfarm to function properly. The backup serverfarm can have a different predictor option than the primary server. When the sticky option is used for a policy, then stickiness can apply to real servers in the backup serverfarm. Once a connection has been balanced to a server in the backup serverfarm, subsequent connections from the same client can be stuck to the same server even when the real servers in the primary serverfarm come back to the operational state. You may allow the sticky attribute when applying the backup serverfarm to a policy.

By default, the sticky option does not apply to the backup serverfarm. To remove the backup serverfarm, you can either use the serverfarm command without the backup option or use the **no serverfarm** command.

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The sorry server (backup server) option was added to this command.

Examples

This example shows how to associate a server farm with a virtual server named PUBLIC_HTTP:

```
SLB-Switch(config-slb-vserver)# serverfarm PUBLIC_HTTP back-up seveneleven sticky
```

Related Commands

serverfarm (Module CSM submode)
reverse-sticky (SLB policy submode)
show module csm vserver redirect
vserver

15856

slb-policy

Use the **slb-policy** command in the SLB virtual server configuration submode to associate a load-balancing policy with a virtual server. Use the **no** form of this command to remove a policy from a virtual server.

slb-policy *policy-name*

no slb-policy *policy-name*

Syntax Description

policy-name	Policy associated with a virtual server.

Defaults

This command has no default settings.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

Multiple load-balancing policies can be associated with a virtual server. URLs in incoming requests are parsed and matched against policies defined in the same order in which they are defined with this command. The policy name must match the name specified in a previous **policy** command.

Note The order of the policy association is important; you should enter the highest priority policy first.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to associate a policy with a virtual server.:

```
SLB-Switch(config-slb-vserver)# slb-policy COOKIE-POLICY1
```

Related Commands

vserver
policy
show module csm owner
show module csm vserver redirect

ssl-sticky

Use the **ssl-sticky** command in the SLB virtual server configuration submode to allow SSL sticky operation. Use the **no** form of this command to remove the SSL sticky feature.

ssl-sticky offset *X* **length** *Y*

no ssl-sticky

Syntax Description

offset	Keyword to specify the SSL ID offset.
X	Sets the offset value.
length	Keyword to specify the SSL ID length.
Y	Sets the length.

Defaults

The default is **offset 0** and **length 32.**

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

This feature allows you to stick an incoming SSL connection based only on this special section of the SSL ID specified by the offset and length values. The **ssl-sticky** command was added to ensure that the CSM always load balances an incoming SSL connection to the SSL Termination Engine that generated that SSL ID.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to associate a policy with a virtual server.:

```
SLB-Switch(config-slb-vserver)# ssl-sticky offset 0 length 32
```

Related Commands

vserver
policy
show module csm owner
show module csm vserver redirect

15854
D

sticky

Use the **sticky** command to ensure that connections from the same client use the same real server. Use the **no** form of this command to change the sticky timer to its default value and remove the sticky option from the virtual server.

sticky *duration* [***group*** *group-id*] [**netmask** *ip-netmask*] [**source** | **destination** | **both**]

no sticky

Syntax Description

duration	Sticky timer duration in minutes; the range is from 1 to 65535.
group	(Optional) Keyword to place the virtual server in a sticky group for connection coupling.
group-id	(Optional) Number identifying the sticky group to which the virtual server belongs; the range is from 0 to 255.
netmask	(Optional) Keyword to specify which part of the address should be used for stickiness.
ip-netmask	(Optional) Network that allows clients to be stuck to the same server.
source	(Optional) Keyword to specify the source portion of the IP address.
destination	(Optional) Destination portion of the IP address.
both	(Optional) Specifies that both the source and destination portions of the IP address are used.

Defaults

The default is **no sticky**. Sticky connections are not tracked.
The group ID default is 0. The sticky feature is not used for other virtual servers.
The network default is 255.255.255.255.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

The last real server that was used for a connection from a client is stored for the *duration* value after the end of the client's latest connection. If a new connection from the client to the virtual server is initiated during that time, the same real server that was used for the previous connection is chosen for the new connection.

A nonzero sticky group ID must correspond to a sticky group previously created using the **sticky** command. Virtual servers in the same sticky group share sticky state information.

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The IP reverse-sticky optional parameters are introduced.

Examples

This example shows how to set the sticky timer duration and places the virtual server in a sticky group for connection coupling:

```
SLB-Switch(config-module-csm)# vserver PUBLIC_HTTP
SLB-Switch(config-slb-vserver)# sticky 60 group 3
```

Related Commands

sticky
sticky-group (SLB policy submode)
reverse-sticky
url-hash
show module csm sticky
show module csm vserver redirect

5852

reverse-sticky

Use the **reverse-sticky** command to ensure that the CSM switches connections in the opposite direction back to the original source. Use the **no** form of this command to remove the reverse-sticky option from the policy or the default-policy of a virtual server.

reverse-sticky *group-id*

no reverse-sticky

Syntax Description

group-id	Number identifying the sticky group to which the virtual server belongs; the range is from 0 to 255.

Defaults

The default is **no reverse-sticky**. Sticky connections are not tracked.
The group ID default is 0. The sticky feature is not used for other virtual servers.
The network default is 255.255.255.255.

Command Modes

SLB virtual server configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The **IP reverse-sticky** command is introduced.

Examples

This example shows how to set the IP reverse-sticky feature:

```
SLB-Switch(config-module-csm)# vserver PUBLIC_HTTP
SLB-Switch(config-slb-vserver)# reverse-sticky 60
```

Related Commands

sticky
sticky-group (SLB policy submode)
show module csm sticky
show module csm vserver redirect

url-hash

Use the **url-hash** command in the SLB virtual server configuration submode to set the beginning and ending pattern of a URL to parse URLs for the URL hash load-balancing algorithm. Use the **no** form of this command to remove the hashing from service.

url-hash {**begin-pattern** | **end-pattern**} *pattern*

no url-hash

Syntax Description

begin-pattern	Keyword to specify the beginning of the URL to parse.
end-pattern	Keyword to specify the ending of the URL to parse.
pattern	Pattern string to parse.

Defaults

The default is **no url-hash**.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

The beginning and ending patterns apply to the URL hashing algorithm that is set using the **predictor** command in the SLB serverfarm submode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to specify a URL pattern to parse:

```
SLB-Switch(config-slb-vserver)# url hash begin pattern lslkjfsj
```

Related Commands

predictor (SLB serverfarm configuration submode)
vserver
show module csm vserver redirect

5850

9

virtual

Use the **virtual** command in the SLB virtual server configuration submode to configure virtual server attributes. Use the **no** form of this command to set the virtual server's IP address to 0.0.0.0 and its port number to zero.

virtual *ip-address* [*ip-mask*] *protocol port-number* [**service ftp** | **rtsp**] [**unidirectional**]

no virtual *ip-address*

Syntax Description

ip-address	IP address for the virtual server.
ip-mask	(Optional) Mask for the IP address to allow connections to an entire network.
protocol	Load-balancing protocol, either TCP, UDP, any, or a number from to 255.
port-number	(Optional) Decimal TCP/UDP port number (0-65535) or port name.
service ftp	(Optional) Keyword to combine connections associated with the same service so that all related connections from the same client use the same real server. FTP data connections are combined with the control session that created them. If you want to configure FTP services, these keywords are required.
service rtsp	(Optional) Keyword to combine connections to the Real Time Streaming Protocol (RTSP) TCP port 554.
unidirectional	(Optional) Sets the data flow to unidirectional.

Defaults

The default IP mask is 255.255.255.255.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

Clients connecting to the server farm represented by the virtual server use this address to access the server farm. This service option is allowed only if a port number is specified. A port of 0 (or **any**) means that this virtual server handles all ports not specified for handling by another virtual server with the same IP address. The port is used only for TCP or UDP load balancing.

The following TCP port names can be used in place of a number:

XOT—**X25** over TCP (1998)

dns—Domain Name Service (53)

ftp—File Transfer Protocol (21)

https—HTTP over Secure Sockets Layer (443)

matip-a—Mapping of Airline Traffic over IP, Type A (350)

nntp—Network News Transport Protocol (119)

pop2—Post Office Protocol v2 (109)

pop3—Post Office Protocol v3 (110)

smtp—Simple Mail Transport Protocol (25)

telnet—Telnet (23)

www—World Wide Web—Hypertext Transfer Protocol (80)

any—Allows traffic for any port, or the same as specifying a 0.

Command History

Release	Modification
1.1(1)	This command was introduced.
2.1(1)	*ip-netmask*, UDP/arbitrary protocol introduced.
2.2.1	RTSP support introduced.
3.1(1)	Added the idle timeout for unidirectional flows feature.

Examples

This example shows how to create a virtual server and assign it an IP address, protocol, and port:

```
SLB-Switch(config-slb-vserver)# virtual 102.35.44.79 tcp 1 unidirectional
```

Related Commands

vserver
show module csm vserver redirect

5848
D

vlan

Use the **vlan** command in the SLB virtual server submode to define which source VLANs may access the virtual server. Use the **no** form of this command to remove the VLAN.

vlan *vlan-number*

no vlan

Syntax Description

vlan-number	VLAN that the virtual server may access.

Defaults

The default is all VLANs.

Command Modes

SLB virtual server configuration submode.

Usage Guidelines

The VLAN must correspond to an SLB VLAN previously created with the **vlan** command.

Command History

Release	Modification
2.1(1)	This command was introduced.

Examples

This example shows how to specify a VLAN for virtual server access:

```
SLB-Switch(config-slb-vserver)# vlan 5
```

Related Commands

show module csm vserver redirect
show module csm vlan
vlan

5847
D-1

xml-config

Use the **xml-config** command to enable XML for a CSM module, and enter the XML configuration submode. Use the **no** form of this command to remove the XML configuration.

xml-config

no xml-config

Defaults

This command has no default settings.

Command Modes

Module CSM configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to display the XML configuration:

```
SLB-Switch(config-module-csm)# xml-config
SLB-Switch(config-slb-xml)#
```

Related Commands

client-group
vlan
client-group
credentials

5846
D.

client-group

Use the **client-group** command in the SLB XML submode to allow only connections sourced from an IP address matching the client group. Use the **no** form of this command to remove the owner.

client-group [*1-99* | *name*]

no client-group

Syntax Description

1-99	(Optional) Client group number.
name	(Optional) Name of the client group.

Defaults

The default is **no client-group**.

Command Modes

SLB XML configuration submode.

Usage Guidelines

When a client group is specified, only connections sourced from an IP address matching that client group are accepted by the CSM XML configuration interface. If no client group is specified, then no source IP address check is performed. Only one client-group may be specified.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to specify a client group:

```
SLB-Switch(config-slb-xml)# client-group domino
```

Related Commands

client-group

credentials

Use the **credentials** command in the SLB XML submode to define one or more username and password combinations. Use the **no** form of this command to remove the credentials.

credentials *user-name password*

no credentials *user-name*

Syntax Description

user-name	Name of the credentials user.
password	Password for the credentials user.

Defaults

This command has no default settings.

Command Modes

SLB XML configuration submode.

Usage Guidelines

When one or more credentials commands are specified, the CSM HTTP server authenticates user access.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to specify the user and password credentials for access:

```
SLB-Switch(config-slb-xml)# credentials savis XXXXX
```

Related Commands

client-group

5844

inservice

Use the **inservice** command in the SLB XML submode to enable XML for use by the CSM. If this command is not specified, XML is not used. Use the **no** form of this command to disable XML.

inservice

no inservice

Defaults

This command has no default settings.

Command Modes

SLB XML configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to enable XML:

```
SLB-Switch(config-slb-xml)# inservice
```

Related Commands

xml-config

port

Use the **port** command in the SLB XML submode to specify the TCP port on which the CSM HTTP server listens. Use the **no** form of this command to remove the port.

port *port-number*

no port

Syntax Description		
	port-number	Sets the CSM port.

Defaults

The default is port 80

Command Modes

SLB XML configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to specify the TCP port for the server:

```
SLB-Switch(config-slb-xml)# port 80
```

Related Commands

client-group

5842
D

vlan

Use the **vlan** command in the SLB XML submode to restrict the CSM HTTP server to accept connections only from the specified VLAN. Use the **no** form of this command to specify that all vlans are accepted.

vlan *id*

no vlan

Syntax Description

id	VLAN name.

Defaults

The default is **no vlan**.

Command Modes

SLB XML configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

This example shows how to specify an owner for virtual server access:

```
SLB-Switch(config-slb-xml)# vlan 9
```

Related Commands

client-group

Apêndice EX

CISCO SYSTEMS

5841
D.

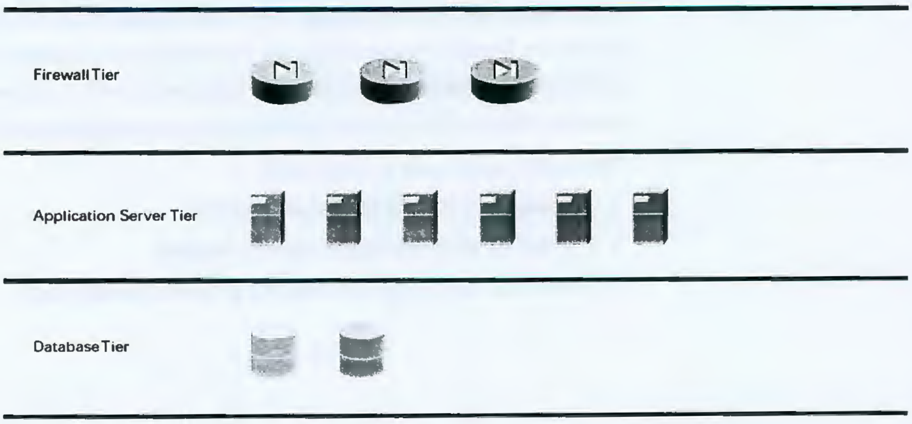
White Paper

Removing Content Switching Performance Barriers: A Discussion of the **Cisco CSM** Pipelined Network Processor Architecture

Introduction

As Web applications become increasingly business-critical—particularly in the areas of e-commerce, customer relationship management (CRM), and employee resource management (ERM) the performance, scalability, security, and availability of the application infrastructure become paramount concerns for IT and network managers. These requirements drive the deployment of Web applications in tiers or layers. Figure 1 shows a typical deployment. In this application, we see a security tier consisting of a layer of firewalls, an application server tier, and a database tier. Each tier may be scaled horizontally by adding additional devices of the appropriate type. As anticipated load on the layer increases, more machines are added to handle the load. In addition, by having multiple devices at each tier, provision is made for functional redundancy. If any device at a given layer fails another device may pick up its work.

Figure 1. Typical Web Application Infrastructure



3840
D

In order for this approach to scaling and failover to work, there must also be a mechanism for intelligently routing messages to and from each of the layers. This is the role fulfilled by content switches. Content switches route messages to individual machines by inspecting the contents of the messages and forwarding them to specific machines based on policies that meet the requirements of the device or application.[1] Content switches monitor the health of each of the devices and provide automatic failover by routing messages to the remaining devices in the tier, this again based on policies set to provide the desired behavior. Because of the critical role they play in enhancing Web application performance, availability, and security, content switches have become an indispensable part of e-business infrastructure.

Network designers building out data centers to support these applications now need to cope with the deployment of firewalls and content switches in addition to their more traditional concerns about routers, LAN switches, and WAN and Internet connectivity. This complexity is accelerating the need for more integrated functions such as firewall and content switching in LAN switches. In addition, the increasing percentage of dynamically generated content in web applications results in a higher load on application servers and databases. This in turn means that a given performance level (in terms of page views or hits per second) requires a greater number of servers, creating greater port density requirements on content switches. The Cisco Content Switching Module for the Catalyst® 6500 Series switch and 7600 Internet router (CSM) was designed to meet these requirements for high density and tight integration with the Layer 2 and Layer 3 infrastructures. In addition, the Cisco CSM sets a new standard for high-end content switching performance. Using a new pipelined network processor architecture, the Cisco CSM achieves better performance by an order of magnitude than previous-generation content switches. The Cisco CSM is especially well suited to deep-packet scanning and inspection operations such as HTTP header matching.[2] In fact, the Cisco CSM turns the Cisco Catalyst 6500 Series switches into the densest, highest performing content switches in the marketplace today—without sacrificing either Layer 2 or Layer 3 performance or burdening the cost of the base platform.

The balance of this paper explores in detail the unique architecture of the Cisco CSM. It will be assumed that the reader has a basic understanding of IP, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Hypertext Transfer Protocol (HTTP) (including Secure Socket Layer [SSL] and the concepts of URLs and cookies). It will also be assumed that the reader has a basic level of understanding about the *role* of content switches in a network but not *how* content switches operate to fulfill this role.[3]

This paper will discuss the following:

- An overview of content switch operation
- Categories of processing in content switches
- The Cisco CSM pipelined network processor architecture

[1] The terms "policy" and "policies" as used in this document should be interpreted to mean a generic set of rules or configurable controls that govern the operation of a content switch. They should not be confused with the configuration instructions or keywords used to implement those policies on specific products.

[2] This is especially significant given the overwhelming use of cookies by application server vendors to preserve user session information across multiple HTTP requests. One of the primary requirements for content switches operating in this tier of the infrastructure is to provide session persistence via inspection of these session cookies. Although most content switch benchmarks today do not take into account cookie processing requirements, it is one of the most taxing operations they are asked to perform. The Cisco CSM is especially well suited for these types of operations.

[3] The reader is referred to the Cisco Content Networking homepage at www.cisco.com/go/contentswitch for more information about content switching and its role in web applications.

An Overview of Content Switch Operation

As previously discussed, the primary role of content switches is to route messages to and from specific devices or machines based upon the requirements of the application as well as the devices themselves. These application and device requirements are expressed in terms of policies that are configured on the content switch. For example, when routing messages to a group of firewalls, one might want to balance the load across the available firewalls while at the same time ensuring that all messages associated with a particular application connection traverse the same firewall in both the forward and reverse direction. This is because the firewalls need to be able to statefully inspect all the packets associated with a connection in both directions. When routing messages to application servers, one might be concerned with balancing the load across the application servers, with the additional constraint that all connections from a particular client get routed to the same point-of-contact application server until a particular transaction or set of transactions is complete.[4]

In general, the set of policies that can be implemented in content switches fall into one of the following broad categories:[5]

1. Load balancing policies—these policies describe how connections and requests are to be distributed across an array of servers that are eligible to receive them. These policies are expressed in terms of the criteria that identify the requests to be distributed, the eligible machines capable of handling those requests, and the algorithm(s) to be used to distribute them across the machines. Examples of load-distribution algorithms include: round robin, weighted round robin, least connections, weighted least connections, least loaded, predictive hash, and others. An example of a load-balancing policy might be the following:

   Policy 1:

   For each inbound request where:

   Destination IP address = 192.32.12.3

   Protocol = TCP

   Destination port = 80 (HTTP)

   Balance the load across the following eligible servers:

   IP address 10.10.10.1, port 80

   IP address 10.10.10.2, port 80

   IP address 10.10.10.3, port 80

   Using the following load distribution algorithm:

   Round Robin

[4] The "point of contact" server is the server selected for the first of a series of connections or transactions. It is typically selected with the goal of balancing the load across all servers. Once this server has been selected, this goal becomes secondary to the goal of maintaining "persistence" between this client and server until the requisite set of connections or transactions is complete.

[5] A detailed discussion of the finer points of content switching policies is beyond the scope of this document. The intent here is merely to convey the types of operations performed by content switches to provide context for our architectural discussion. The reader is referred to the CSM documentation for more information.

5838
D.

2. Persistence policies—these policies describe requirements to keep a series of connections or requests coming to the same server in the array until a particular transaction or unit of work is complete. With persistence policies there must be some token passed in each request that can be used by the content switch as the means for maintaining persistence. These tokens are most often IDs that represent a specific server or user session. They are typically found encoded in a URL or cookie or, in the case of secure traffic, in the unique SSL session ID. An example of a persistence policy might be the following:

   Policy 2:

   For each inbound request where:

   Destination IP address = 192.32.12.3

   Protocol = TCP

   Destination port = 80 (HTTP)

   Balance the load across the following eligible servers:IP address 10.10.10.1, port 80

   IP address 10.10.10.2, port 80

   IP address 10.10.10.3, port 80

   Using the following load distribution algorithm:

   Round Robin

   Maintain persistence to selected server using the following token:

   Cookie = “Session-ID”

Note: Note that the persistence policy works in conjunction with a load-balancing policy. The load-balancing policy is used to select the initial point-of-contact server. The server then sets the “Session-ID” cookie to a unique value for this session. The persistence policy alerts the content switch to monitor the setting of this cookie and to maintain an association between this cookie and the point-of-contact server so that subsequent requests received with this cookie are directed to the same server.

3. Server failure policies—these policies are designed to give the operator control over switch behavior in the event of server failure. One can envision, for example, different applications requiring different kinds of treatment. This is particularly true when using persistence policies as described above. What should be done when a server that has a persistent client connection mapped to it fails mid-transaction? Possible options include: reset the connection, issue an HTTP redirect (perhaps to a server that displays an error message), rebalance the connection to a new server using the load-balancing policy, or direct to a special "sorry server" that becomes active if there are no other eligible servers for this policy. An example of a server failure policy follows:

   Policy 3:

   For each inbound request where:

   Destination IP address = 192.32.12.3

   Protocol = TCP

   Destination port = 80 (HTTP)

   Balance the load across the following eligible servers:

   IP address 10.10.10.1, port 80

   IP address 10.10.10.2, port 80

   IP address 10.10.10.3, port 80

   Using the following load distribution algorithm:

   Round Robin

   Maintain persistence to selected server using the following token:

   Cookie = "Session-ID"

   Upon persistent server failure:

   Issue HTTP redirect to 192.32.15.1/failuremessage.htm

5836 D

4. Content-specific policies—these policies are used to specify different treatment for different types of content. One might want to direct all requests for cacheable content, for example, to a set of reverse proxy caches that offload the processing of static images from application servers. Or one might want to partition a web server farm into static and dynamic sections. The following is an example of a content specific policy.

   Policy 4:

   For each inbound request where:

   Destination IP address = 192.32.12.3

   Protocol = TCP

   Destination port = 80 (HTTP)

   URL = "*.GIF, *.JPEG" /* file extensions for cacheable image types

   Balance the load across the following eligible caches:

   IP address 10.10.20.1, port 80

   IP address 10.10.20.2, port 80

   IP address 10.10.20.3, port 80

   Using the following load distribution algorithm:

   URLHash

Note: The URLHash distribution mechanism results in a more optimal cache replacement policy by keeping requests for the same image files on the same caches.

5. Device-specific policies—these policies are used to specify different treatment for different types of devices. Perhaps one wants to direct clients using wireless devices to a set of servers that customize content for that device's specific formatting requirements. Below is an example of a device-specific policy that accomplishes this goal.

   Policy 5:

   Destination IP address = 192.32.12.3

   Protocol = TCP

   Destination port = 80 (HTTP)

   User agent contains the string "Palmscape/PR5" /* Browser = Palm V

   Balance the load across the following eligible wireless gateways:

   IP address 10.10.30.1, port 80

   IP address 10.10.30.2, port 80

   IP address 10.10.30.3, port 80

   Using the following load distribution algorithm:

   Round Robin

5835
D.

Virtual Servers, Real Servers, NAT, and Dispatch Modes

There are a few characteristics of these policies that are worthy of special note. First, note in the above examples that a policy matches a particular destination address, protocol, and port. This information, which represents the servers behind the content switch to the outside world, is known as the virtual server definition. In fact, the Cisco CSM allows a virtual server to consist of an arbitrary range of IP addresses (including all IP addresses), an IP protocol number, a TCP or UDP port number, and an incoming virtual LAN (VLAN).[6]

The actual servers to which connections are forwarded are known as real servers.[7] These are defined by their IP addresses and ports. Content switches essentially accept connections that match virtual servers and direct them to real servers. In the process of doing so, they may modify the packets they forward as follows.

Content switches employ two modes of forwarding: Network Address Translation (NAT) mode (also called directed mode) and dispatch mode. In NAT or directed mode, the destination address is translated[8] from the received destination (the one that matched the virtual) to the address of the target real server. The MAC address is also rewritten. In dispatch mode, only the MAC address is rewritten, and the original destination IP address is preserved. This latter mode is important in order to load balance devices such as firewalls that are designed to transparently screen the traffic but are not necessarily the end recipients of it.[9]

In fact, content switches are commonly required to modify additional fields in packets they forward. In addition to the destination address and MAC address information already cited, common examples include source IP addresses, source and destination ports, sequence numbers, and checksums.

Policies, Protocol Layers, and Delayed Binding

New connections that arrive at a content switch are first classified to determine whether matching policies exist and then processed according to the actions specified by those policies. In the set of policy examples above, Policy 1 is invoked if the destination IP address = 192.32.12.3, the protocol = TCP, and the destination port = 80 (HTTP). The classification of this connection, therefore, can take place at Layers 3 and 4 (IP address, protocol, and port). This classification can take place completely on the initial packet of the TCP connection (the SYN packet).

[6] Valid values for protocol, port, and VLAN include "any" which indicates that the rule will match any value in that field. The VLAN identifier is useful for applying different actions to identical matching criteria based on the ingress VLAN. This is particularly useful for firewall load-balancing applications as well as for transparent caching applications. VLAN identification is also generally useful for security purposes or to separate different networks (such as a service provider environment where the same Cisco CSM is shared among different customers). See the CSM documentation for details.

[7] Real servers are logical constructs separate from physical servers. A real server is identified by an IP address and port. A physical server can host multiple real servers, for example, each represented by a unique IP address and port number combination.

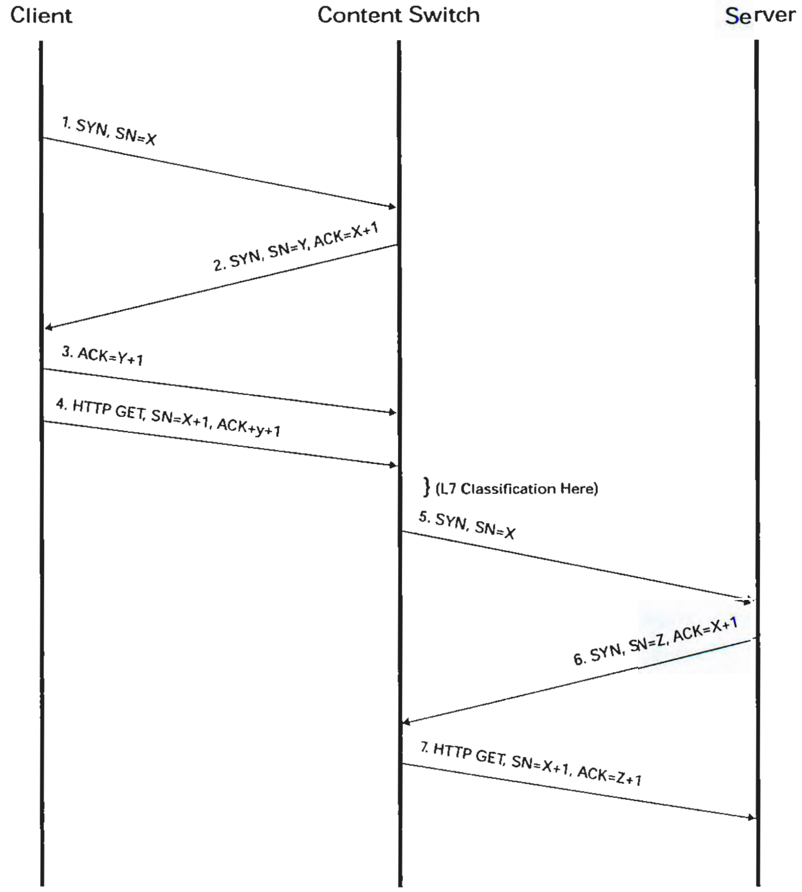
[8] NAT implies that the destination and/or source IP address is translated to a new address. In addition, dependent IP header information (such as the header checksum) will be changed as well.

[9] Dispatch mode has also been used with lower-performing content switching devices, including the Cisco Local Director as well as some third-party content switches. The goal in these types of configurations is to load balance traffic in the client-to-server direction while removing the content switch from the path of traffic in the server-to-client direction. This eliminates the content switch as a bottleneck in the direction of greatest traffic flow. However, this mode of operation significantly complicates and constrains the configuration. For example, loopback addresses must be configured on all the servers, servers must be Layer 2-adjacent to switch, and Address Resolution Protocol (ARP) is turned off on servers. The high performance of the Cisco CSM for both Layer 4 and Layer 7 load balancing effectively removes all motivation to use dispatch mode other than those mentioned above.

5834
D.

Look again at policy examples two through five above. Each of these policies requires additional classification based on data contained in the HTTP header. In examples two and three, the required info is in the "Cookie" header, in example four, the "URL," and in example five, the "User-Agent" header. Because HTTP is considered an application-layer protocol, classification at this layer is referred to as "Layer 7" classification.[10] In order for the classification of these connections and requests to take place properly, a process commonly known as "delayed binding" is used by the content switch to obtain the Layer 7 information required to classify the connection.

Figure 2. Delayed Binding Used for Layer 7 Classification



[10] Layer 7 is the OSI reference model application layer. There is a long-standing debate as to whether this should be called "Layer 5" classification due to the fact that TCP/IP only has five layers, with the fifth being the application layer. While technically incorrect "Layer 7" is the commonly used title.

Delayed binding deals with a "catch 22" situation. The content switch cannot apply Layer 7 policy to the connection until it has received the initial HTTP request and its associated headers (URL, Cookies, User-Agent, etc.) but the client will not send the HTTP information until it believes it has a connection established with the server. The content switch acts as a temporary proxy for the connection until it receives sufficient information to apply its policy, then binds the connection to the correct server as the policy dictates—hence the term "delayed binding." Figure 2 illustrates the process of delayed binding used for Layer 7 classification.

In steps one through three, we see the client establishing a TCP connection with the content switch as a proxy for the server. In step four, the client sends its HTTP request. The content switch now has sufficient data to apply its Layer 7 policy (in this case resulting in the selection of a specific server). In steps five through seven, the content switch establishes a connection with the selected server and forwards the HTTP GET on to that server.[11]

Sequence Number Remapping

The process of delayed binding introduces an additional piece of complexity to the forwarding process—sequence number remapping. For TCP connections, each participating party is responsible for establishing their own initial sequence number. The sequence number is then incremented by one for each byte transmitted over the connection. The receiver is responsible for sending back acknowledgements for each byte received.[12] Because the content switch is acting as a proxy for the initial connection, it must supply an initial sequence number for its side of the connection. The initial sequence number established by the real server is different. This implies that the content switch must translate these sequence numbers in both directions for all packets transferred. In Figure 2, note the sequence numbers and acknowledgments for all participants (client, content switch, and server). In particular, note that the initial sequence number selected by the content switch is different from the initial sequence number set by the server. The content switch must compute the difference between these two initial sequence numbers and maintain that relationship by remapping the sequence numbers for each packet transferred in both directions.[13]

HTTP 1.1 and Connection Remapping

To this point, the terms "connection" and "request" have been used somewhat interchangeably. One might infer from this that there is a one-for-one relationship between HTTP requests and connections. In fact, for earlier versions of HTTP this was true. With the introduction of HTTP 1.1, however, it is possible to transfer a series of HTTP requests and responses over a single TCP connection. For certain types of applications such as caching applications (see discussion on Policy 4 above), one might desire to send each of the requests to a different server based on the load-balancing policy. In these applications it will be necessary to maintain the client side of the connection while "remapping" the server side of that connection to a new server. The content switch is responsible for correctly terminating the old server side connection, re-computing all of the appropriate NAT, port, and sequence number translations that will be applied to the new connection, establishing a connection with the new server, sending the

[11] A valid policy action may be to drop this connection, in which case steps five through seven will never occur. A TCP reset may be issued to the client in this case.

[12] A detailed discussion of the operation of TCP is beyond the scope of this document. For more information please see Richard Stephens' excellent series entitled *TCP/IP Illustrated*, published by Addison Wesley.

[13] The observant reader will have noticed a few of the finer points of this interaction. First, during the delayed binding phase the number of packets exchanged between client and content switch (4) is greater than the number of packets exchanged between content switch and server (3). This is because the TCP specification allows the acknowledgement to be accompanied by data, a fact the content switch takes advantage of. Second, in this example, the client sequence number is preserved without modification from client all the way to server. This is because it is the server side of the connection that is being proxied by the content switch during the delayed binding process.

5832
D

new HTTP request, and then translating all the appropriate fields of subsequent packets associated with the connection in both directions. Effectively, the Layer 7 classification and the server side of the delayed binding process is repeated for each new HTTP request (steps five through seven in Figure 2).[14] The CSM allows the operator to specify whether connection remapping should be turned on or off for a given virtual server. In the event connection remapping is disabled, Layer 7 policy is applied only to the first in the sequence.

Health Checking

Is it important for content switches to detect the failure of servers or processes and route around them. In complex web applications, one might want to verify several layers of infrastructure upon which a target server depends to complete its function (such as a web server, application software, or database) before sending requests to that server. In order to determine that various pieces of application infrastructure are up and available, content switches need to provide flexible capabilities to test various types of servers. There are two different types of health checking offered in the Cisco Catalyst 6500 CSM: active health checking and inband health checking. Active health checking implies that the content switch is actually sending messages to the servers and looking for certain expected results in return. Active health checking is useful for more complex types of verification, such as verifying availability of the database that a particular Java Servlet relies upon to perform its function. Scripting functions also allow the operator to customize active health checking for applications for which canned capabilities don't exist. Active health checks are sent at regular intervals. Failure of the health check results in labeling a particular server or set of servers unavailable. As with all active techniques of this kind, there is a trade-off between the frequency at which health checks are sent (and how quickly a failure can be detected) and the processing requirements associated with them.

With inband health checking, the content switch actually looks at responses to live requests and can immediately take servers out of service if they fail. Inband health checking is a superior means of detecting physical server and process failures on machines to which the content switch is directly communicating. Because the content switch monitors every active connection, it is possible to detect failures much more rapidly than with active health checking. However, the more complex types of health checking are not possible using this mechanism. In practice, it makes sense to leverage both types of capabilities—inband health checks to detect hard server and process failures and active health checks to verify all components required for a particular application are available.[15]

Categories of Processing in Content Switches

Having briefly reviewed content switch operation, this paper now considers the specific types of processing going on inside content switches as they perform these functions. In general, the various tasks to be performed by content switches fall into one of the following three categories:

- Connection processing
- Forwarding processing
- Control processing

Following is a brief description for each as well as an introduction to the types of performance metrics, which will be useful in comparing different content switch architectures.

[14] If the classification indicates the same server may be used for this request as the previous then no remapping is performed. This allows the application to benefit from HTTP 1.1 persistence as appropriate.
[15] Inband health checking is something for which the Cisco CSM is especially well suited due to its superior connection processing capabilities.

Connection Processing

Connection processing may be viewed as any processing associated with the establishment of new connections, the modification of existing connections, or the tearing down of completed connections. Following is a partial list of tasks that can be considered part of connection processing:

- *Detection of new connections:* Is this packet a TCP SYN or a UDP frame with a 5-Tuple for which there is no forwarding state? If so, we may want to set up a connection.
- *Virtual server lookup:* Does this frame match a configured policy in the content switch? If so, can the switch apply its policy yet or does the switch need to do a delayed binding to get Layer 5 information?
- *Delayed binding:* Perform the 3-way handshake and look at the received Layer 7 data. Does this match a configured policy? If so, apply the policy action.
- *TCP state machine and denial of service detection:* The content switch must ensure that packets it is processing are part of a valid TCP connection. This is required both for error-detection purposes as well as to detect any well known denial-of-service attempt that exploits TCP vulnerabilities.
- *Policy matching:* Parse through the Layer 7 data for the required fields and determine whether those fields match the policy database.
- *Frame buffering:* Sometimes the Layer 7 data is not in the first application frame received. This requires the content switch to buffer frames until a match or no-
- match decision can be made.
- *Server selection:* In most applications, the configured policy action will require the selection of a server based on factors such as load balancing, persistence, and failover requirements.[16] The content switch must determine the server based on these requirements.
- *Determine packet transformations:* Should this connection be NATed? Do sequence numbers need to be translated? The content switch must determine which transformations need to be applied and what they are. The connection processing function must inform the forwarding process function of the connection parameters and transformations.
- *Handle new HTTP requests on HTTP 1.1 connections:* For HTTP 1.1 connections in flight, the content switch must detect new HTTP requests and determine whether a new policy action needs to be taken (such as selecting a new server). This also involves recomputing all packet transforms and ensuring the forwarding process is updated with the new information.
- *Manage server side connections:* For connections where delayed binding has been applied, the content switch must perform the correct 3-way handshake with the server, handling correctly any TCP errors. Likewise, for HTTP 1.1 connection remapping functions, the content switch must correctly terminate the old connections and establish the connection to the new server.
- *Inband health checking:* When inband health checking is turned on, the content switch must monitor server response traffic for failure conditions and take servers out of service as appropriate.
- *Terminate connections:* Connections may terminate normally (when a TCP FIN or RESET is received) or abnormally (a server, client, or something in the network path fails so that no packets are received for some timeout period). The content switch must clean up all state and reclaim all resources consumed by the connection.

[16] Other valid policies may involve dropping specific connections, redirecting specific connections, or forwarding to a specific next-hop router.

Connection Processing Performance:

The following metric is most commonly used when looking at connection processing performance:

- *Connections per second (CPS):* For Layer 4 TCP and UDP traffic, this is the rate at which new connections may be processed. For Layer 7 HTTP traffic, this is the rate at which new connections may be established or existing connections modified (as with HTTP 1.1 connection remapping).[17] Note that connection processing does not take place on every packet associated with every connection, rather it takes place only on those packets associated with the beginning and ending of connections as well as on those that signal the potential need for modification of connections in flight. Applications that make use of long-lived connections and few connection modifications will have lower connection processing requirements than those that are short lived or are modified frequently.

Forwarding Processing

Any processing associated with the forwarding of packets that are part of established connections may be viewed as forwarding processing. Following is a partial list of tasks associated with forwarding processing:

- *Classify packets:* Is this packet part of an existing connection? If not, hand the packet over to the connection-processing function. If so, get packet transformation information, next hop, and quality of service (QoS) and type of service (ToS) information.
- *Apply packet transformations:* Including any address changes, port changes, sequence number changes, checksum changes, ToS changes, and Diffserv changes.
- *Queue and transmit packet at required QoS level:* Send the packet on to its destination.

Forwarding Processing Performance:

The following performance metrics are important when discussing forwarding performance:

- *NAT forwarding rate in packets per second (PPS):* As is true for LAN switching, the number of packets per second that can be forwarded is important. Shorter packet sizes require greater packet-per-second handling capacity for a given throughput. Unlike most LAN switches, content switches are typically performing a significant number of packet transformations, or NAT, on the packets they forward.
- *NAT throughput (Mbps):* Likewise, total NAT throughput in megabits per second (irrespective of packet size) should be understood.
- *Simultaneous connections:* Due to the packet transformations that need to be applied (which are unique for each connection), each connection managed and forwarded by a content switch requires its own forwarding table entry and connection state. Every content switch will therefore have a limit (typically due to forwarding table memory size) to the number of simultaneous connections it can manage.[18]

Note that forwarding processing takes place on every packet the content switch must handle, so although this processing is less complex than the processing associated with connection management and control, it happens more frequently. As we shall see, this processing path should be optimized.

[17] Note to testers- as with most performance metrics, this one can be deceiving. The processing associated with matching a simple URL regular expression such as /* will not be the same as that associated with matching a session cookie, for example. Be sure you are making accurate comparisons.

[18] It is important to make accurate comparisons here. Some vendors will talk about connections as uni-directional entities, others as bi-directional entities. The numbers quoted for Cisco CSM capacity in this paper are bi-directional.

5829
D.

Control Processing

Control processing refers to all other processing that is not associated with either connection setup or forwarding but is nonetheless essential to the proper operation, configuration, monitoring, or control of these processes. Control processing is generally asynchronous to the main tasks of the content switch (such as handling connections and forwarding). A partial list of tasks associated with control processing is as follows:

- *System management processes:* Tasks associated with management of configuration files, system images, booting, diagnostics, care and feeding of hardware, and more.
- *Operations management processes:* Tasks associated with management of the running system, including configuration (such as command line, web interface, and application programming interfaces), statistics and Management Information Base (MIB) management, and Simple Network Management Protocol (SNMP).
- *Active health checking:* Scheduling and transmission of health check messages, examining results, moving servers in and out of service as required. The processing associated with this can be quite extensive and includes the following:
  - Formatting queries
  - Establishing and maintaining connections
  - Transmitting and receiving messages
  - Parsing and interpreting replies
  - Taking appropriate action (which may involve notification of several other parts of the system)

Control-Processing Performance:

The following are useful metrics to consider when discussing control-processing performance:

- *Probes per second (PPS):* The number of probes (or active health check messages) a content switch can process per second. Note that processing requirements increase as active health checks become more complex (such as with scripting).
- *Number of probes:* There will typically be memory or configuration limits to the number of health checks that can be configured.

Note that probes have the lowest frequency of all the processing types discussed, yet because of their complexity they may have the highest unit overhead.[19]

Now that the reader is familiar with how content switches operate and the different categories of processing they must perform, this paper will turn to the details of the Cisco CSM architecture—an architecture that is tuned to the specific types of processing tasks that content switching requires.

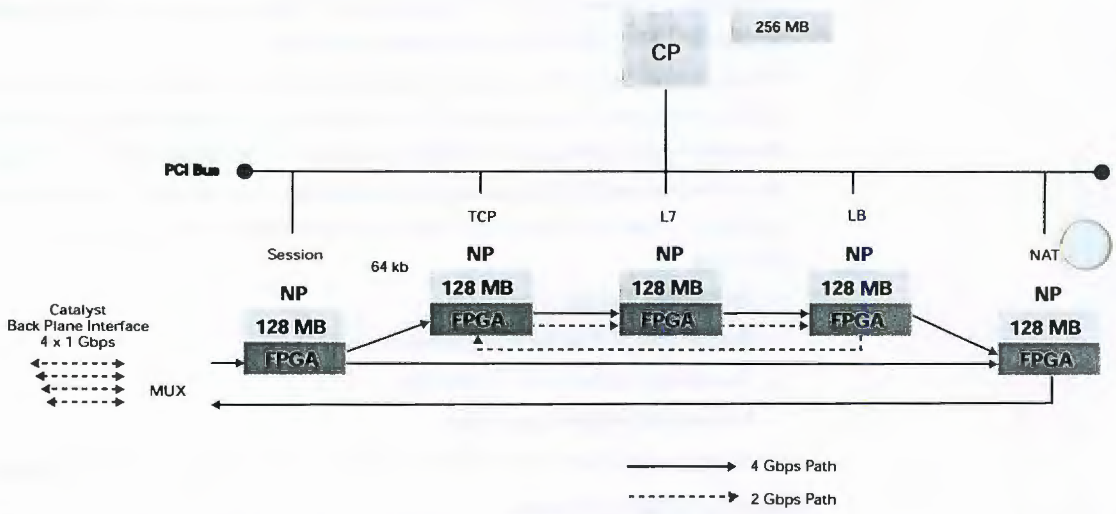
[19] Note also that this is a strong motivation for inband health checking; however, the additional processing overhead associated with it must be factored into connection processing requirements.

5828
D

The Cisco CSM Pipelined Network Processor Architecture

The Cisco CSM hardware architecture consists of a series of five field programmable gate arrays (FPGAs) and network processors (NPs), matched in pairs and structured as a dual pipeline (more on this shortly). Figure 3 illustrates the layout of the FPGA and network processor pairs.

Figure 3. CSM Layout



The Cisco CSM has four 1-Gbps, full-duplex connections to the Cisco Catalyst 6500 backplane, which are muxed together to provide a 4-Gbps, full-duplex data path to the CSM processing complex. From a network standpoint, the CSM is configured to participate in and listen to a set of VLANs on the Cisco Catalyst 6500 backplane. Traffic targeted to the CSM arrives via one or more of the 1-Gbps backplane connections shown. Inputs from the backplane are muxed together to present the CSM processing logic with an aggregate 4-Gbps stream of packets. Once processing begins, a packet matching configured policies will traverse one of two 4-Gbps paths through the processing complex. The first is the connection-processing pipeline. The second is the forwarding pipeline. A detailed discussion of these pipelines will be presented in the next section.

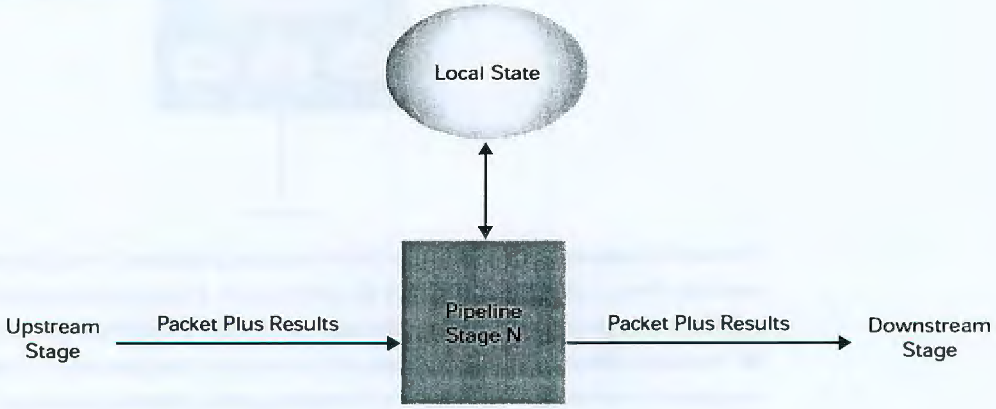
Before moving on to this discussion, a few additional details of the above diagram bear explaining. The first is the separate 2-Gbps path between the pipeline stages labeled TCP, L7, and LB. This path is used for upstream communication between stages. The second is the small chunk of memory (64 KB) shown between the session and TCP pipeline stages. This provides a high-speed, memory-mapped communication path between these stages designed to support high-volume communication.

Each network processor has a connection via a PCI bus to the control processor. The control processor is responsible for the configuration and management of all components on the CSM as well as for the processing associated with certain control tasks (such as active health checking).

Pipeline Overview

The Cisco CSM pipelines consist of a series of linked stages. Each stage consists of a FPGA and network processor pair with associated memory. As packets move through the pipeline, a specific set of operations is performed at each stage. The results of each pipeline stage are then passed along with the packet to the next stage that utilizes those results, the packet itself, and any state it maintains locally about the connection as inputs into its processing. Figure 4 illustrates this idea.

Figure 4. A Pipeline Stage



Note: Each stage of the pipeline may update its own local connection state.

FPGAs

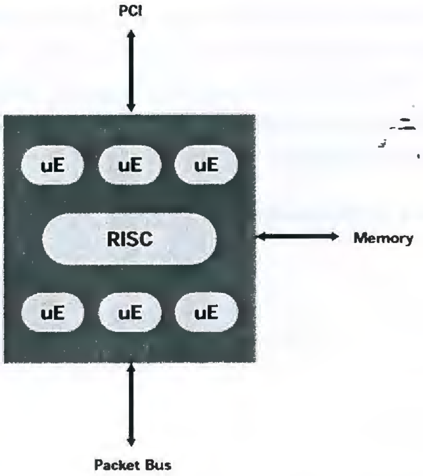
The FPGAs provide an addressable communications fabric between the pipeline stages. Each stage in the pipeline is responsible for determining the downstream stage that should receive the packet next. Note that a stage may "skip" a downstream stage by inserting the address of a further downstream stage as the recipient of its output. Intervening FPGAs at skipped stages merely forward the packet on to the next FPGA unmodified. The network processor at a skipped stage does not see the packet. In this way, latency, bandwidth, and overhead through the system is reduced by bypassing unnecessary processing steps in hardware.

The session-and NAT-stage FPGAs have a few additional functions, which will be explained in the detailed discussion of pipeline stages ahead.

Network Processors

Each network processor has six RISC microengines plus a RISC core, providing a total of over one billion instructions per second. Altogether the network processor pipeline provides over five billion instructions per second, and each network processor has its own dedicated 128-MB pool of high-speed memory. Figure 5 illustrates the Intel IXP 1200 network processor used in the Cisco Catalyst 6500 CSM.

Figure 5. The Intel IXP 1200



The various tasks associated with a particular stage are partitioned across the microengines (uE) in such a way as to maximize the parallelization offered by this architecture. Pipelining maximizes system performance for operations applied to a single packet as it moves through the pipeline. Parallelization maximizes the performance of the system for the many different unrelated packets and connections being processed at the same time. Together they provide exceptional processing performance for forwarding and connection processing.

The Connection and Forwarding Pipelines

Figures 6 and 7 illustrate the connection and forwarding pipelines respectively.

A few observations:

- All packets move through the pipeline in the same direction, entering through the mux from the backplane and leaving through the mux to the backplane.[20]
- There are two stages in common for both pipelines: the "session" stage, and the "NAT" stage.
- It is the session stage that determines which pipeline path the packet will take.

[20] Not all packets that enter will leave because some policies will result in packets being dropped. Other packets may be intended for the module itself (such as ARP, ICMP, and keepalive responses). These are forwarded to the control processor

Figure 6. The Connection Pipeline

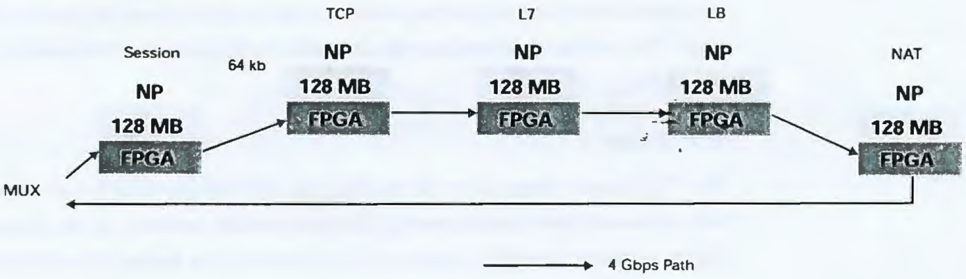
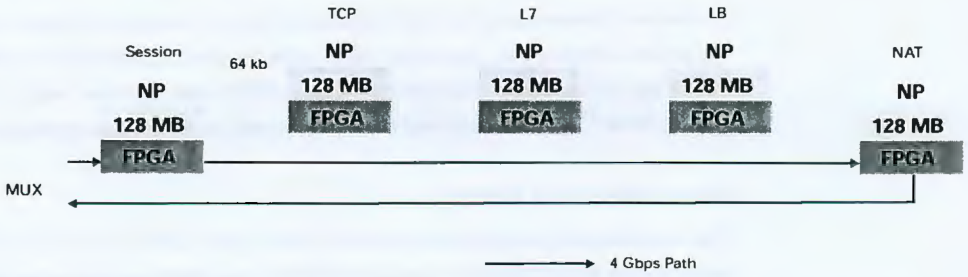


Figure 7. The Forwarding Pipeline



Recalling the earlier discussion about connection and forwarding processing, it is apparent that connection processing is a relatively less frequent task than forwarding processing. This is because connection processing is needed only for the start of connections, the end of connections, and modifications to connections. Packets associated with these events need to be handled differently than those packets that are merely parts of established connections. These only need to be forwarded in accordance with the policy (such as NAT or QoS). The rationale behind the dual pipeline of the Cisco Catalyst 6500 CSM now becomes evident as well: Packets associated with connection-related events are forwarded along the connection pipeline, while packets associated with established connections are forwarded along the forwarding pipeline. Once connections are established, associated packets may be "cut through" along the forwarding pipeline until some new connection-modifying event occurs. This results in much lower processing overhead in the system for the vast majority of packets that must simply be forwarded in accordance with the configured policy.

Following is a brief discussion of each of the individual pipeline stages.

Session Stage

It is the responsibility of the session stage to determine whether the packet indicates the beginning of a connection, the end of a connection, or is part of an existing connection. Packets that are part of an existing connection need only be forwarded over the dedicated 4-Gbps connection to the NAT stage. The connection ID passed with the packet assists the NAT module in quickly locating the correct session entry containing the appropriate packet transformations.

For packets that are determined to require connection processing, the session stage forwards the packet over the connection pipeline path to the TCP stage.

15824

It was mentioned earlier that the session FPGA has some unique functions. The session FPGA essentially preprocesses the received packet for the session network processor. The session network processor receives only that portion of the information from the packet relevant to its decision about the pipeline path selection in an easily digestible form. This substantially reduces the amount of processing that the session network processor has to do to classify the packet.

TCP Stage

The TCP stage is responsible for maintaining TCP session state for all connections. It determines the beginning and end of connections (communicating this information upstream to the session stage), filters denial-of-service attacks, performs delayed binding if required, and forwards the packet on to either the Layer 7 or the load-balancing stage as required.[21]

Layer 7 Stage

Packets are forwarded by the TCP stage to the Layer 7 stage if the Layer 3 and Layer 4 information obtained from the packet indicates that this packet needs to be matched against Layer 7 policies. The Layer 7 stage must parse the packet for relevant fields (such as cookies and URLs) and applies a high-performance regular expression match against them.[22] Packets and results are then passed on to the load-balancing stage.

Load-Balancing Stage

The load-balancing stage receives packets from either TCP or Layer 7 as well as information regarding the virtual server match for this packet. The load-balancing module then applies the configured load-balancing algorithm, persistence policy, or failover policy to the packet. The load-balancing stage then forwards the packet and NAT transformation information to the NAT stage.

NAT Stage

The final stage in the pipeline is the NAT stage, which is responsible for applying all relevant packet transformations to the packets and sending them back to the mux for transmission to the backplane. The NAT stage is also responsible for statistics gathering.

It was previously mentioned that the NAT-stage FPGA had a unique function to perform. Basically this amounts to muxing the inputs received from both pipeline paths and presenting the combined input to the NAT network processor.

[21] Here one sees the benefits of making the FPGAs addressable. The Layer 7 stage can be bypassed for connections that only need processing at Layer 3 or Layer 4.

[22] The regular expression-matching capability of the Cisco CSM itself is quite sophisticated in that not just suffix (*.something) and prefix (something*), but any type of regular expression can be configured, using typical notations (such as range of characters, question marks to indicate a fixed amount of generic characters, negation, OR, and AND). There is no significant impact on the performance when matching against a complex regular expression as opposed to a simple one. See CSM documentation for details.

Control Processing

All control-processing tasks (see above discussion) take place on a dedicated RISC processor within the Cisco Catalyst 6500 CSM. This approach provides dedicated processing cycles for these tasks, enabling the system to scale in terms of control task volume or complexity (such as for active health checking) without negatively impacting performance for connection or forwarding processing.[23]

Cisco Catalyst 6500 CSM Architecture Evaluation

The Cisco Catalyst 6500 CSM architecture makes use of a number of innovative techniques to push content switching to new levels of price performance. Its primary innovation is in the areas of the connection and forwarding pipelines used for connection and forwarding processing respectively. By leveraging the parallel processing capabilities of the selected network processors in a pipeline, the architecture is capable of delivering remarkable performance in both categories. Through the use of a dedicated control processor the architecture performs admirably in this area as well.

The Cisco Catalyst 6500 CSM sets a new standard for content switching in the following dimensions:

- *Features:* The programmability of the selected components yields tremendous flexibility in feature development. The performance offered by the pipeline architecture makes it possible to consider features that were heretofore impractical, such as inband health checking, return error code checking, and deep regular expression matching.
- *Price and performance:* In this dimension the Cisco Catalyst 6500 CSM is without peer, delivering NAT forwarding performance of 4 Gbps and connection performance at rates exceeding 150,000 connections per second. The Cisco Catalyst 6500 CSM can support almost one million simultaneous bi-directional connections. For customers with the highest performance requirements, no other solution will prove as cost-effective.[24]
- *Port density:* A Cisco Catalyst 6500 with CSM can have as many as 528 10/100 ports.
- *Integration with Layer 2 and Layer 3 infrastructure:* Because the Cisco Catalyst 6500 CSM runs in the Cisco Catalyst 6500 with Cisco IOSÒ Software, customers are assured of the highest level of integration with their Layer 2 and Layer 3 infrastructure. They can leverage the industry-leading QoS, Layer 2, and Layer 3 features of the Cisco Catalyst 6500 including any of the network interfaces supported in the Cisco Catalyst 6500 such as packet over SONET (POS) and 10 Gigabit Ethernet modules.

Integration with other data center capabilities: The Cisco Catalyst 6500 CSM supports integrated firewall, intrusion detection, VPN, and in the future, other capabilities as well.

The Cisco Catalyst 6500 CSM is one of several products in the Cisco content switching product line addressing the growing customer demand for scalable Layer 4 to Layer 7 services as a complement to their existing Layer 2 and Layer 3 infrastructure. Cisco content switches enable businesses to build highly available and secure network data centers in support of their Internet and intranet applications. The Cisco Catalyst 6500 CSM provides an integrated services module for the Cisco Catalyst 6500 Series switches and Cisco 7600 Series Internet routers and delivers the highest Layer 4 to Layer 7 performance along with a rich set of application features. The Cisco content switch

[23] The Cisco CSM control processor is separate from the management processor located on the supervisor in the Cisco Catalyst 6500 Series switch itself. The Cisco Catalyst 6500Series switch provides most of the management functions for the Cisco CSM through Cisco IOSÒ Software, such as configuration, command line, and SNMP. The Cisco CSM control processor is therefore free to perform other control tasks such as active health checking.

[24] The Cisco CSM is currently being used with success in the largest production networks, some with server farms in excess of 500 servers driving peaks loads of over 50,000 connections per second and 2 Gbps of NAT throughput.

product line also includes the Cisco CSS 11000 Series content services switches and, the most recent addition to the product line, the Cisco CSS 11500 Series content services switches, which offer a compact modular platform with rich Layer 4 to Layer 7 services for e-business applications.

For more information on Cisco content switching, please visit

http://www.cisco.com/go/contentswitch

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice EZ

CiscoWorks LAN Management Solution 2.2 Introduction

CiscoWorks LAN Management Solution (LMS) provides a robust set of applications for maintaining, monitoring, and troubleshooting a broad range of devices in an end-to-end Cisco AVVID (Architecture for Voice, Video and Integrated Data) network. Built upon popular Internet-based standards, CiscoWorks LMS enables network operators to more efficiently and effectively manage the network through a simplified browser-based interface that can be accessed anytime from anywhere within the network. Taking advantage of a Web-based client/server architecture, CiscoWorks LMS can be easily integrated with other popular network management systems or other third-party management solutions running in the network.

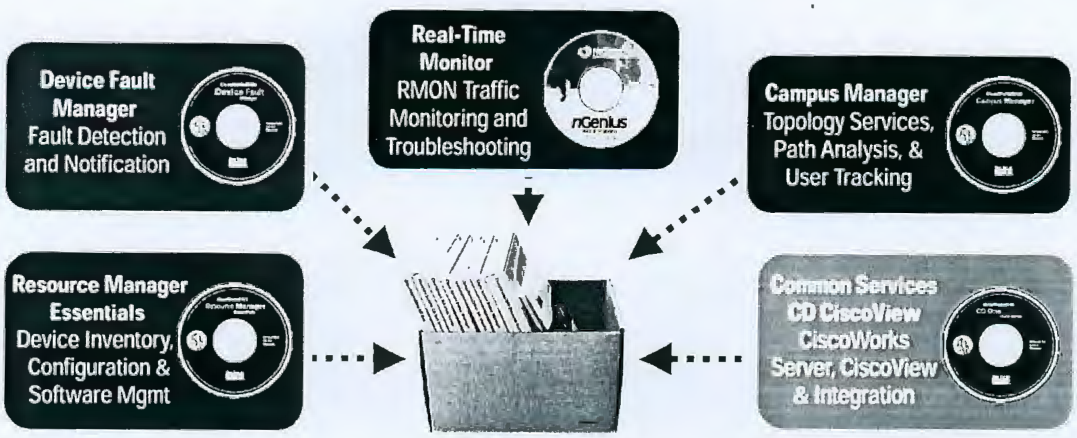
CiscoWorks LMS provides a solid foundation of basic and advanced management applications that complement CiscoWorks products. Other CiscoWorks products include the CiscoWorks Routed WAN Management (RWAN) Solution, which addresses the needs of the WAN with response time and access list management. The IP Telephony Environment Monitor (ITEM) ensures the readiness and manageability of converged networks that support voice over IP (VoIP) and IP telephony traffic and applications. The Cisco VPN/Security Management Solution (VMS) provides an integrated set of Web applications with features that assist in the deployment and monitoring of virtual private network (VPN) and security devices. Together, CiscoWorks products offer leading-edge solutions for improving the accuracy and efficiency of your operations staff, increasing overall availability of your network through proactive planning and maximizing network security.

The Changing Campus LAN

A key part of the business infrastructure, today's LANs are critical systems. The management of local-area networks has evolved from being device centric, to now focusing on managing the convergence of both data and voice traffic over a common infrastructure. As a result, it has become increasingly important to isolate, troubleshoot, and monitor network devices so that connections and services are always available. CiscoWorks LMS delivers advanced discovery technologies, port assignment tools, sophisticated connectivity analysis, configuration management tools, and device and network diagnostic capabilities (including fault management and Remote Monitoring [RMON] traffic monitoring) to help manage the complexities of a converged network.

A Comprehensive Solution

CiscoWorks LMS combines applications and tools for configuring, monitoring, and troubleshooting the campus network. Designed to address the networks powered by Cisco today, it also provides a flexible framework to address the device management needs of networks converging voice, video, and data; networks being protected with Cisco SAFE Blueprint for network security technologies; and networks designed for content migration.


Device Fault Manager
Fault Detection and Notification
Real-Time Monitor
RMON Traffic Monitoring and Troubleshooting
nGenius
Campus Manager
Topology Services, Path Analysis, & User Tracking
Resource Manager Essentials
Device Inventory, Configuration & Software Mgmt
Common Services
CD CiscoView
CiscoWorks Server, CiscoView & Integration

The CiscoWorks LMS consists of operationally focused tools. These tools include fault management, scalable topology views, sophisticated configuration, Layer 2/3 path analysis, voice-supported path trace, traffic monitoring, end-station tracking workflow application servers management, and device troubleshooting capabilities.

CiscoWorks LMS is built on the CiscoWorks common services foundation. This design facilitates operations workflow between applications by linking data collection, monitoring, and analysis tools—all from a single desktop application. For example, a user complaint of slow response time or a poor IP phone connection can be quickly diagnosed using CiscoWorks LMS Layer 2 path tools that automatically acquire user path information stored in one database, and highlight devices on a topology map. Additionally, switch or router configurations can then be quickly examined, or RMON traffic data can be reviewed to detect anomalies or the need for changes. Those actions may draw information from one or more applications.

CiscoWorks LMS uses Internet standards to tie together best-of-breed tools and to take advantage of their capabilities through data and task integration standards. Using the common information model (CIM) and Extensible Markup Language (XML), the industry standards for data-sharing CiscoWorks LMS offers a means of extracting data and using it with popular network management platform products. With the CiscoWorks LMS, Cisco offers a complete family of dedicated hardware Cisco Catalyst® network analysis modules (NAMs). Cisco Catalyst NAMs provide increased visibility into switched LAN environments comprising 10/100 and Gigabit Ethernet links for comprehensive, end-to-end, seven-layer monitoring of network infrastructures.

Solution Components

The following applications are included in CiscoWorks LMS:

- CiscoWorks Campus Manager—CiscoWorks Campus Manager is a suite of Web-based applications designed for managing networks powered by Cisco switches. These include Layer 2 device and connectivity discovery, workflow application server discovery and management, detailed topology views, virtual LAN/LAN Emulation (VLAN/LANE) and ATM configuration, end-station tracking, Layer2/3 path analysis tools, and IP phone user and path information.
- CiscoWorks Device Fault Manager—CiscoWorks Device Fault Manager provides real-time fault analysis for Cisco devices. It generates "intelligent Cisco traps" through a variety of data collection and analysis techniques. These can be locally displayed, e-mailed, or forwarded to other popular event management systems.
- nGenius Real-Time Monitor—The nGenius Real-Time Monitor is a Web-enabled multiuser traffic management tool set that provides access to network-wide, real-time RMON information for monitoring, troubleshooting, and maintaining network availability. Its applications graphically report and analyze device, link, and port level RMON collected traffic data from RMON-enabled Cisco Catalyst switches and internal network analysis module.
- CiscoWorks Resource Manager Essentials (RME)—CiscoWorks RME provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis.
- CiscoView—CiscoView is a Web-based tool that graphically provides real-time status of Cisco devices. The tool can drill down to display monitoring information on interfaces and access configuration functions.
- CiscoWorks Management Server—The CiscoWorks Management Server provides the common management desktop services and security across the CiscoWorks Family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications.

Key Functions and Applications

Table 1 gives key functions and applications of the CiscoWorks LMS.

Table 1 CiscoWorks LAN Management Solution Key Application/Function

	Product	Management Benefit
Offers intelligent, automatic discovery of Cisco devices to create topology views of the network	CiscoWorks Campus Manager	The Cisco Campus Manager Topology Services functionality discovers Cisco devices and calculates Layer 2 relationships to provide views of the Cisco network by ATM domain, VTP[1] domain, LAN edge view, and a general Layer 2 view.
Gives topology status indications	CiscoWorks Campus Manager	The topology maps indicate the discovery and SNMP[2] status of Cisco devices; these maps also are launching points for other CiscoWorks applications.
Configures, manages, and monitors VLAN[3] and ATM services/networks	CiscoWorks Campus Manager	CiscoWorks Campus Manager provides tools for creating, deleting, and editing VLANs; it provides ATM tools for displaying virtual circuits and for configuring SPVCs/SPVPs.[4]

Table 1 CiscoWorks LAN Management Solution Key Application/Function

	Product	Management Benefit
Discovers end stations and IP phones connected to switch ports and identifies user locations based on user ID	CiscoWorks Campus Manager	The CiscoWorks Campus Manager User Tracking functionality correlates MAC[5] address and IP address to switch port; integration with Microsoft's PDC and Novell's NDS tree provides the user ID for even more efficient user location and tracking.
Traces Layer 2 and Layer 3 connectivity between two points (devices, servers, phones) in the network	CiscoWorks Campus Manager	The CiscoWorks Campus Manager Path Analysis tool performs path analysis for Layer 2 and Layer 3 devices using the device host name or IP address, and shows results on a map display, in a table display, or in a trace display.
Intelligently analyzes fault conditions designed to detect problems before they become network disruptions	CiscoWorks Device Fault Manager	CiscoWorks Device Fault Manager automated fault detection recognizes common problems in networks without forcing users to define their own rules sets, SNMP trap filters, or device polling intervals.
Interprets fault conditions at both the device and VLAN levels	CiscoWorks Device Fault Manager	With the characteristics of over a 100 Cisco routers and switches predefined, new device support is easily added via Cisco.com. Cisco Device Fault Manager simplifies managing both Layer 2 and Layer 3 environments.
Collects RMON/RMON2 statistics from LAN switches, NAMs, and legacy Cisco SwitchProbe® devices	nGenius Real-Time Monitor	nGenius Real-Time Monitor monitors LAN traffic for protocols, applications, and interfaces to apply appropriate filters, reducing costs and increasing performance.
Provides for LAN troubleshooting at network and application packet levels	nGenius Real-Time Monitor	nGenius Real-Time Monitor helps resolve network and application issues by providing total network visibility from the application layer down to the data link layer for virtually any topology that exists today.
Offers detailed software and hardware inventory reporting	Cisco RME	Cisco RME provides accurate Cisco inventory baseline information, including memory, slots, software versions, and boot ROMs needed to make decisions about the network.
Offers automated update engines for device software and configuration changes	Cisco RME	Cisco RME allows software and configuration updates to be sent to selected devices on a scheduled basis; it reduces time and errors involved in network updates.
Offers a consolidated troubleshooting tools device center	Cisco RME	A wide collection of switch and router analysis tools is accessible from a single location; third-party applications can link to the device center.
Offers centralized change audit logging	Cisco RME	A comprehensive change-monitoring log records users and applications that are active on the network.
Offers graphical device management	CiscoView	CiscoView displays a browser representation of Cisco router and switch devices, color-coded to indicate operational states, with access to configuration and monitoring tools.

Table 1 CiscoWorks LAN Management Solution Key Application/Function

	Product	Management Benefit
Provides application access security	CiscoWorks Server	The CiscoWorks desktop controls user access to applications, ensuring that only appropriate classes of users can access tools that change network parameters versus read-only tools.
Offers third-party integration tools (Integration utility)	CiscoWorks Management Server	The CiscoWorks Management Server simplifies the Web integration of third-party and other Cisco management tools.

1. Virtual Trunking Protocol
2. Simple Network Management Protocol
3. Virtual LAN
4. Soft permanent virtual circuits/soft permanent virtual paths
5. Media Access Control

Key Functions and Applications

Deployment Options

Consider the following when installing the CiscoWorks LAN Management Solution:

- All applications do not have to be installed initially; applications not installed initially may be installed later.
- Most applications require the CiscoWorks Management Server from the Common Services CD (formerly CD One), which must be installed first.
- The CiscoWorks Campus Manager application depends on CiscoWorks RME, which is included as part of the CiscoWorks LAN Management Solution.

All solutions can coexist on the same server if they support and operate with the services of Common Services 2.2. However, network managers may want to consider such factors as the number of applications hosted, system resources, and number of devices to be managed in determining if all or a subset of the solutions are installed on the same server.

CiscoWorks solutions offer deployment flexibility. System administrators should use the guidelines given previously when planning the deployment of the various solution bundles. Some components within a solution require the CiscoWorks Management Server and must be installed on that machine. CiscoView and nGenius Real Time Monitor software can be set up on an independent server. The placement of components is a function of performance requirements and the size of the network.

Server System Requirements

Hardware/Operating System

UNIX

- System: Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) running Solaris 2.8 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM for workstations, 2-GB RAM for servers, 8-MB e-cache

- Available disk: 40-GB internal FC-AL disk drive for workstation and dual drives of this type for server configurations

Windows

- System: IBM PC compatible with 550-MHz or higher Pentium III processor running Microsoft Windows 2000 Advanced Server (with Terminal Services turned off), Server or Professional Edition with Service Pack 2 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM
- Available disk: 40 GB with 2-GB swap recommended

Note: These system requirements are based on managing 500 devices with CiscoWorks RWAN and LAN Management solutions loaded on a single server. Refer to the Installation documentation for more information on required operating system patches.

Client Browser System Requirements

Hardware/Operating System

UNIX

- System: Sun Ultra 10 running Solaris Version 2.7 or 2.8
- System: HP9000 Series running HP-UX 11.0
- System: IBM RS/6000 workstation running AIX 4.3.3
- Memory: 256 MB

Windows

- System: IBM PC-compatible computer with 300-MHz or higher Pentium processor running Windows XP Professional, Windows 2000 (Advanced Server, Server or Professional) with Service Pack 3
- Memory: 256 MB

Note: Refer to the installation documentation for more information on required operating system patches.

Web Browser

UNIX

- Solaris: Netscape v4.76
- HP-UX: Netscape v4.78, 4.79
- AIX: Netscape v4.78, 4.79

Windows

- Windows 2000/XP: Netscape v4.78, 4.79
- Windows 2000/XP: Internet Explorer v6.0.26

Note: Refer to the Installation documentation for more information on required operating systems patches, browser plug-ins, or Java Virtual Machine (JVM) versions.

Service and Support

CiscoWorks products are covered by the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 7 x 24 access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A Cisco SAS contract ensures that customers have easy access to the information and services needed to stay up-to-date with newly supported device packages, patches, and minor updates. For further information on service and support offerings, contact your local sales office.

Ordering Information

The CiscoWorks LAN Management Solution includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris Workstation/Server. The products within this solution can be combined with other CiscoWorks products if they support the same CiscoWorks Management Server version, operating environment, and system requirements. Contact your local Cisco representative for available white papers and documentation outlining best practices for implementing a CiscoWorks management solution architecture.

To place an order, contact your Cisco sales representative.

Refer to the CiscoWorks LAN Management Solution individual product data sheets for more information on operating environment and system requirements.

For More Information

For more information on the CiscoWorks LAN Management Solution, visit http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2425/index.html.

5845

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

DOC, 000233

CPL/AC

PREGÃO
050/2003

LOCAÇÃO DE
EQUIPAMENTOS
DE INFORMÁTICA
INCLUINDO
ASSISTÊNCIA
TÉCNICA E
TREINAMENTO

HP INVENT –
MANUAL
APÊNDICES FA A
FZ

2003
PASTA 11

Apêndice FA

CISCO SYSTEMS

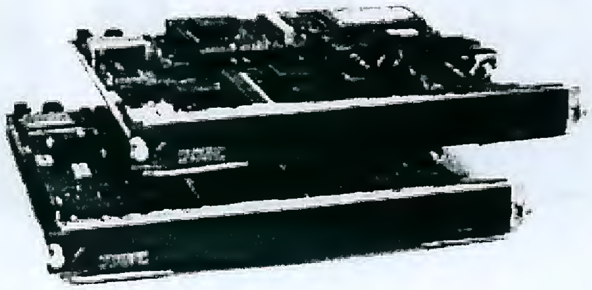
Data Sheet

Cisco Catalyst 6500 Series and Cisco 7600 Series
Network Analysis Module 1 and 2

Second-Generation, High-Performance Network Analysis Modules for Cisco Catalyst 6500 Series and Cisco 7600 Series

Cisco Systems®, the worldwide leader in networking for the Internet, addresses the need for multiservice network management and traffic monitoring in high-capacity switched Ethernet LANs and routed WANs with a new generation of the Network Analysis Module (NAM) for Cisco® Catalyst® 6500 Series switches and Cisco 7600 Series routers. The NAM is an integrated and powerful traffic monitoring service module that occupies a single slot in the chassis and enables network managers to gain application-level visibility into network traffic with the ultimate goal of improving performance, reducing failures, and maximizing returns on network investments.

The second-generation NAMs are available in two hardware versions, NAM-1 and NAM-2, and offer high performance monitoring and crossbar (fabric) connectivity to meet diverse network analysis needs in scalable switching and routing environments running at gigabit speeds. The NAMs come with an embedded, Web-based traffic analyzer, which provides full-scale remote monitoring and troubleshooting capabilities that are accessible through a Web browser.



Application-Level Visibility Built into the Network

The NAMs give network managers visibility into all layers of network traffic by providing application-level Remote Monitoring (RMON) functions based on RMON2 and other advanced Management Information Bases (MIBs). The NAMs add to the built-in Remote Monitoring (mini-RMON) features in Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers that provide port-level traffic statistics at the Media Access Control (MAC) or data link layer. The NAMs provide intelligence to analyze traffic flows for applications, hosts, conversations, and network-based services such as quality of service (QoS) and voice over IP (VoIP).

Integrated Monitoring for LANs and WANs

The NAMS use several data sources from local and remote switches and routers to provide combined visibility into LAN and WAN environments. The NAMs collect data from physical ports, virtual LANs (VLANs), or Cisco EtherChannel®

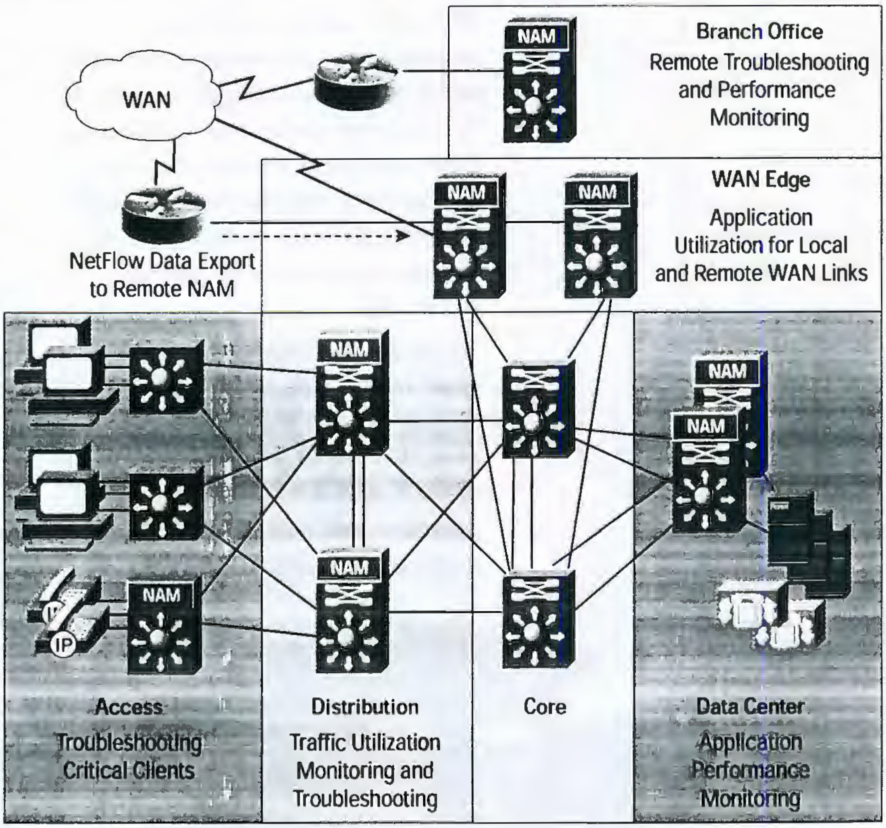
connections using the Switch Port Analyzer (SPAN) feature. For selective monitoring of large amount of traffic or for traffic from WAN interfaces, VLAN access control list (VACL)-based captures can be used to filter traffic before it is sent to NAM. In addition, the NAMs collect and analyze NetFlow Data Export from local and remote devices to provide broad application-level visibility into the network, including remote WAN segments. The NAMs also collect data from remote switches using the remote SPAN (RSPAN) feature of the Cisco Catalyst switches.

Flexible Deployment Scenarios

The NAMs can be deployed in the Cisco Catalyst 6500 Series at LAN aggregation points (for example, in the core or distribution layer) for proactive monitoring; at service points (for example, in data centers, server farms, or Cisco CallManager clusters in IP telephony networks) where performance is critical; and at important access points (critical clients, IP phone closets) where quick troubleshooting is required. They can also be deployed in Cisco 7600 Series routers at WAN edges or in Catalyst 6500 Series switches connected to WAN routers. When deployed at remote branch offices, the NAMs provide unique advantage to perform remote troubleshooting and traffic analysis through its Web-based Traffic Analyzer without having to send personnel or to haul large amounts of data to the central site. Figure 1 highlights the deployment of NAMs to enable comprehensive traffic monitoring and analysis for performance monitoring, troubleshooting, and capacity planning.

Figure 1

Deploying NAMs to Build Intelligence into the Network to serve a Variety of Applications

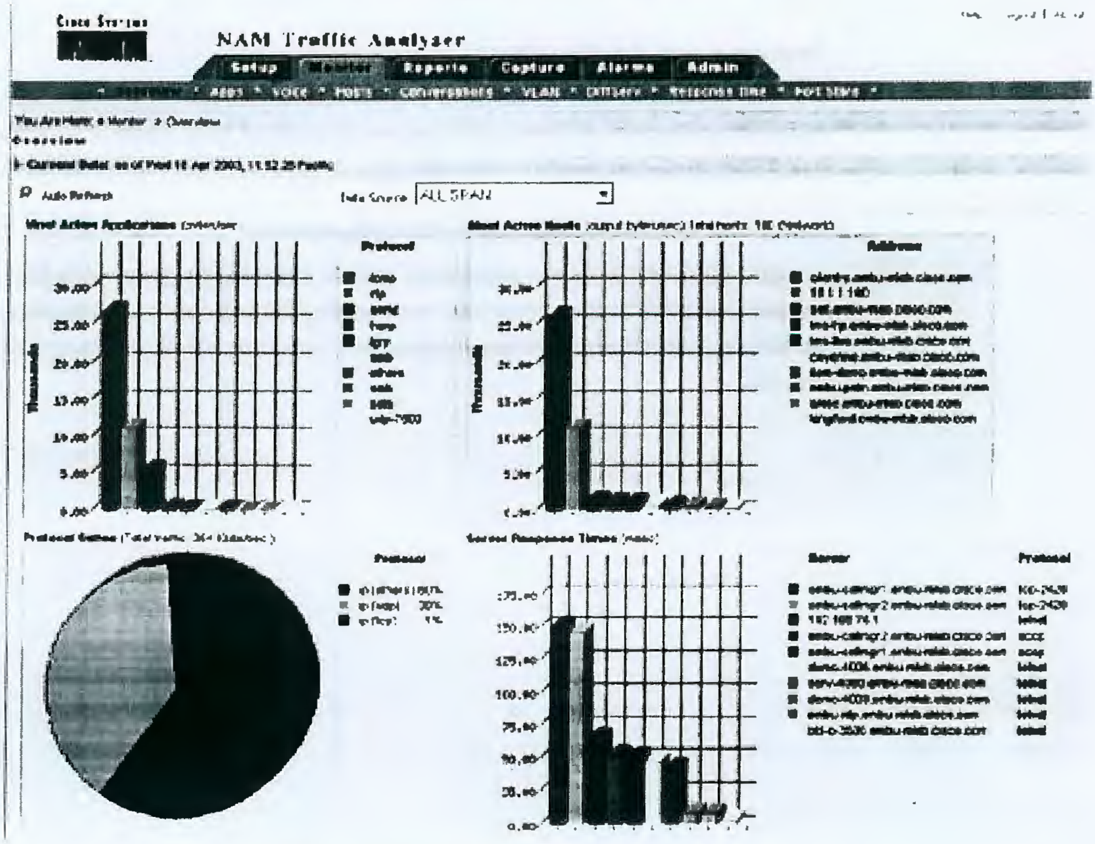

WAN
NAM
Branch Office
Remote Troubleshooting and Performance Monitoring
NAM
NAM
WAN Edge
Application Utilization for Local and Remote WAN Links
NetFlow Data Export to Remote NAM
NAM
NAM
NAM
NAM
NAM
IP
IP
Access
Troubleshooting Critical Clients
Distribution
Traffic Utilization Monitoring and Troubleshooting
Core
Data Center
Application Performance Monitoring

Easy to Deploy and Use

The NAMs come with the embedded, Web-based Traffic Analyzer with extensive monitoring and troubleshooting capabilities. Because the NAMs integrate monitoring functions directly into the switch and have complete data collection and data analysis capabilities on board, they are easy to deploy and managers can conveniently access data from anywhere using a Web browser (Figure 2). For security, users can be given role-based access and the Web-browser access can be secured with up to 168-bit encryption.

Figure 2

Web-Based Traffic Monitoring for both LAN and WAN with the embedded NAM Traffic Analyzer



The NAMs also provide the flexibility to use standards-based external applications using the Simple Network Management Protocol (SNMP). NetScout *n*Genius Real-Time Monitor, a component of the CiscoWorks LAN Management Solution (LMS), collects data from NAMs across the network and provides reports on traffic flow.

Major Benefits

- Increase return on network investment—The visibility provided by the NAMs enables better utilization of network resources to meet business objectives. They ease deployment of network-based services and help in capacity planning.
- Reduce productivity loss and revenue loss—Through proactive monitoring and quick troubleshooting capabilities, the NAMs prevent loss due to network degradation and downtime.
- Enhance network security—The NAMs provide investigation and verification capabilities to supplement other security mechanisms such as intrusion detection and firewalls. They can also be used to detect threats by watching anomalies in the network traffic.

Features and Applications

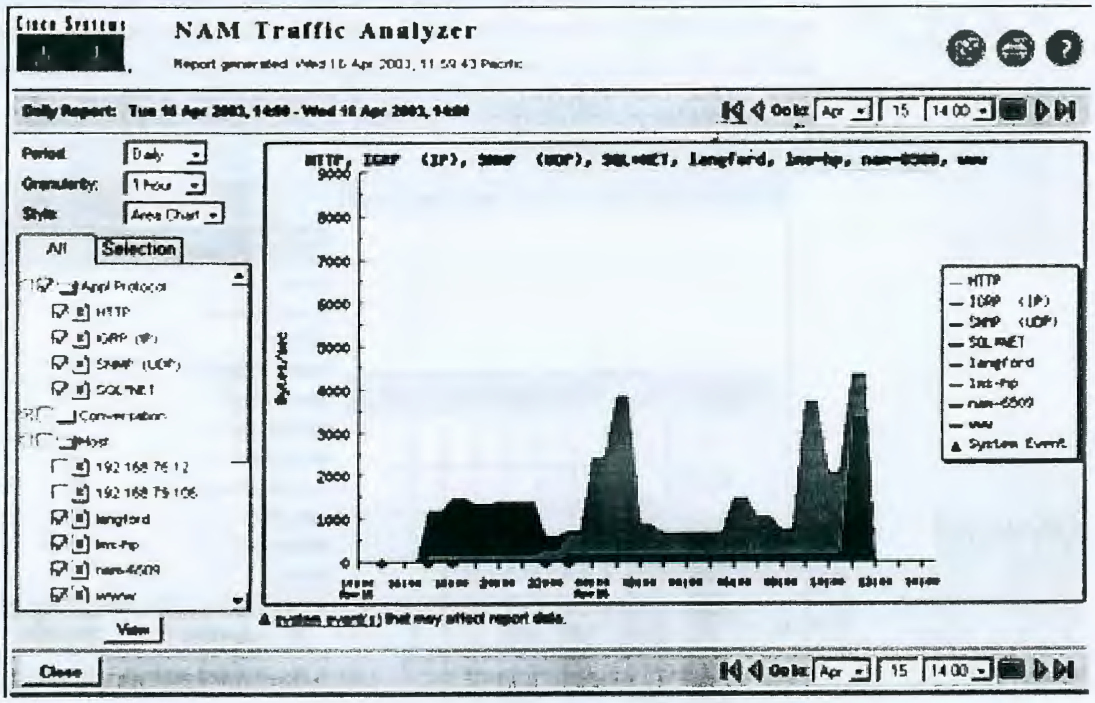
The data collected by the NAMs can be used for several vital management activities, including real-time and historical application monitoring, performance management, fault isolation, troubleshooting, and capacity planr The NAMs also play an active role in managing differentiated services such as voice.

Real-Time and Historical Application Monitoring

Using RMON, RMON2, several extended RMON MIBs, and NetFlow, the NAMs detect the applications on the network and provide detailed real-time and historical information about how these applications utilize the bandwidth, which hosts access those applications, and which client/server pairs generate the most traffic (Figure 3A and 3B).

Figure 3A

Monitoring Applications and Hosts on the Network



Cisco Systems

NAM Traffic Analyzer

Report generated: Wed 16 Apr 2003, 11:59:43 Pacific

Daily Report: Tue 15 Apr 2003, 14:00 - Wed 16 Apr 2003, 14:00

Go to: Apr 15 14:00

Period: Daily

Granularity: 1 Hour

Style: Area Chart

All | Selection

- ☑ Appl Protocol
  - ☑ HTTP
  - ☑ IGRP (IP)
  - ☑ SNMP (UDP)
  - ☑ SQL*NET
- □ Conversation
- □ Host
  - □ 192.168.75.12
  - □ 192.168.75.105
  - ☑ langford
  - ☑ lnx-hp
  - ☑ nam-6509
  - ☑ www

View

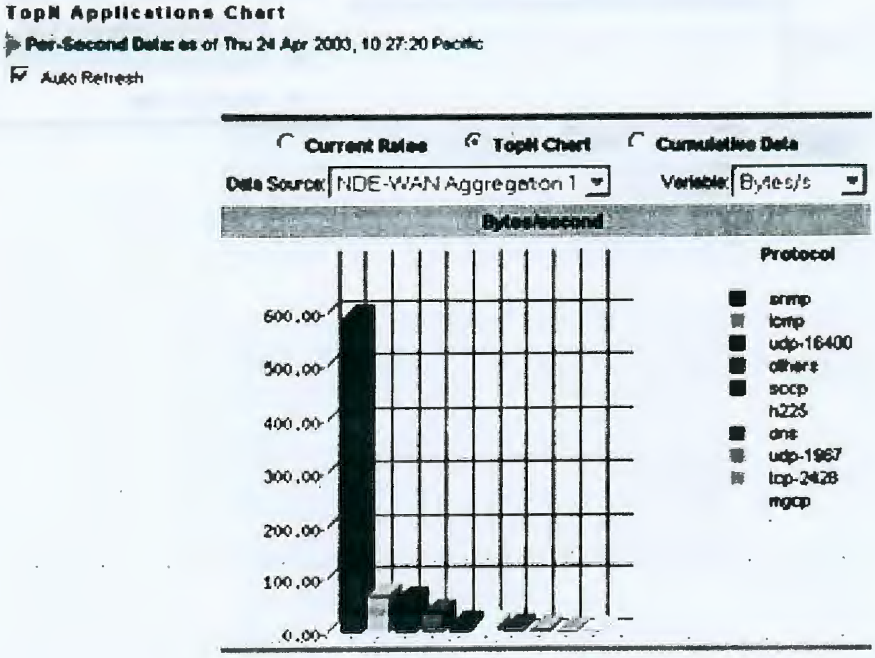
▲ system event(s) that may affect report data.

Close

Go to: Apr 15 14:00

Figure 3B

Monitoring Application Utilization on a WAN link using NetFlow Data Export from a Remote Router



TopN Applications Chart

Per-Second Data: as of Thu 24 Apr 2003, 10:27:20 Pacific

☑ Auto Refresh

○ **Current Rates** ● **TopN Chart** ○ **Cumulative Data**

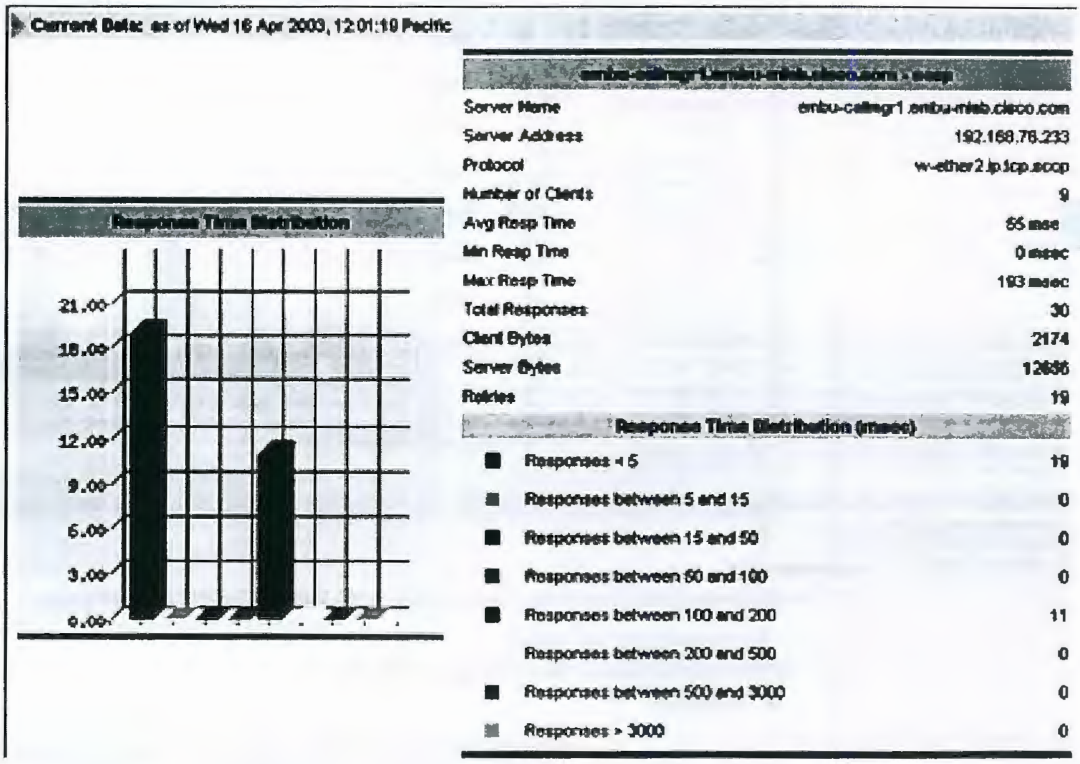
Data Source: NDE-WAN Aggregation 1

Variable: Bytes/s

Performance Management

The NAMs provide valuable information about the delays in server responses to client requests. Using the Application Response Time (ART) MIB, developed by Cisco partner NetScout Systems, the NAMs can identify problems with applications or servers in critical environments such as e-commerce and IP telephony (Figure 4).

Figure 4
Application Response Time Monitoring



Current Data: as of Wed 16 Apr 2003, 12:01:19 Pacific

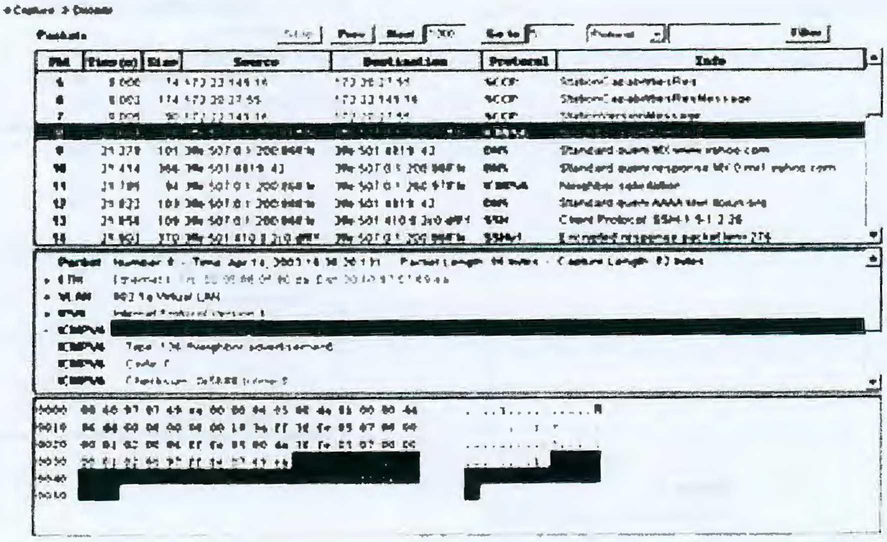
embu-callmgr1.embu-mlab.cisco.com - sccp	
Server Name	embu-callmgr1.embu-mlab.cisco.com
Server Address	192.168.76.233
Protocol	w-ether2.ip.tcp.sccp
Number of Clients	9
Avg Resp Time	65 msec
Min Resp Time	0 msec
Max Resp Time	193 msec
Total Responses	30
Client Bytes	2174
Server Bytes	12686
Retries	19

Response Time Distribution (msec)		
■	Responses < 5	19
■	Responses between 5 and 15	0
■	Responses between 15 and 50	0
■	Responses between 50 and 100	0
■	Responses between 100 and 200	11
	Responses between 200 and 500	0
■	Responses between 500 and 3000	0
■	Responses > 3000	0

Fault Isolation and Troubleshooting

Using the NAMs, network managers can set thresholds and alarms on various network parameters such as increased utilization, severe application response delays, and voice quality degradation, and be alerted to potential problems. The NAMs provide comprehensive views on applications, hosts, voice, quality of service (QoS), and so on, to isolate faults or malfunctions in the network. The NAM Traffic Analyzer can capture and decode packets in real time to aid troubleshooting (Figure 5).

Figure 5
Capturing and Decoding Packets with NAM



No.	Time (s)	Size	Source	Destination	Protocol	Info
5	[illegible]	74	[illegible]	[illegible]	SCCP	StationCapabilitiesReq
6	[illegible]	174	[illegible]	[illegible]	SCCP	StationCapabilitiesResMessage
7	[illegible]	90	[illegible]	[illegible]	SCCP	StationVersionReqMessage
8	[illegible]	[illegible]	[illegible]	[illegible]	ICMPv6	[illegible]
9	[illegible]	101	[illegible]	[illegible]	DNS	Standard query MX www.yahoo.com
10	[illegible]	[illegible]	[illegible]	[illegible]	DNS	Standard query response MX [illegible] yahoo.com
11	[illegible]	94	[illegible]	[illegible]	ICMPv6	Neighbor solicitation
12	[illegible]	[illegible]	[illegible]	[illegible]	DNS	Standard query AAAA [illegible]
13	[illegible]	[illegible]	[illegible]	[illegible]	SSH	Client Protocol: SSH-[illegible]
14	[illegible]	[illegible]	[illegible]	[illegible]	SSHv1	Encrypted response packet len=[illegible]

```
Packet   Number 8 - Time Apr 10, 2003 [illegible]   Packet Length [illegible] bytes - Capture Length [illegible] bytes
+ ETH    Ethernet II [illegible]
+ VLAN   802.1q Virtual LAN
+ IPv6   Internet Protocol Version 6
- ICMPv6
  ICMPv6   Type: 136 (Neighbor advertisement)
  ICMPv6   Code: 0
  ICMPv6   Checksum: [illegible]
```

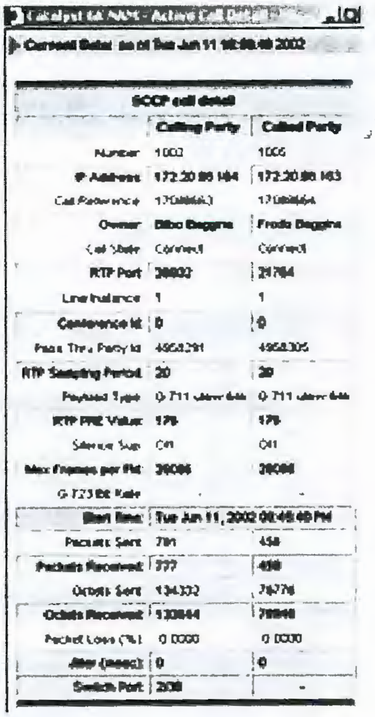
```
0000  [illegible]
0010  [illegible]
0020  [illegible]
0030  [illegible]
0040
0050
```

VoIP and QoS Monitoring

The NAMs can analyze voice traffic flows in real time to collect valuable information, including call setup details and voice quality metrics. Network managers can be alerted to voice quality degradation and can isolate potential problems (Figure 6).

The NAMs make the deployment of QoS for voice and other critical services effective by identifying violations of QoS policies. The NAMs support the Differentiated Services Monitoring (DSMON) MIB, which monitors traffic by differentiated services code point (DSCP) allocations defined by QoS policies (Figure 7).

Figure 6
IP Telephony Monitoring



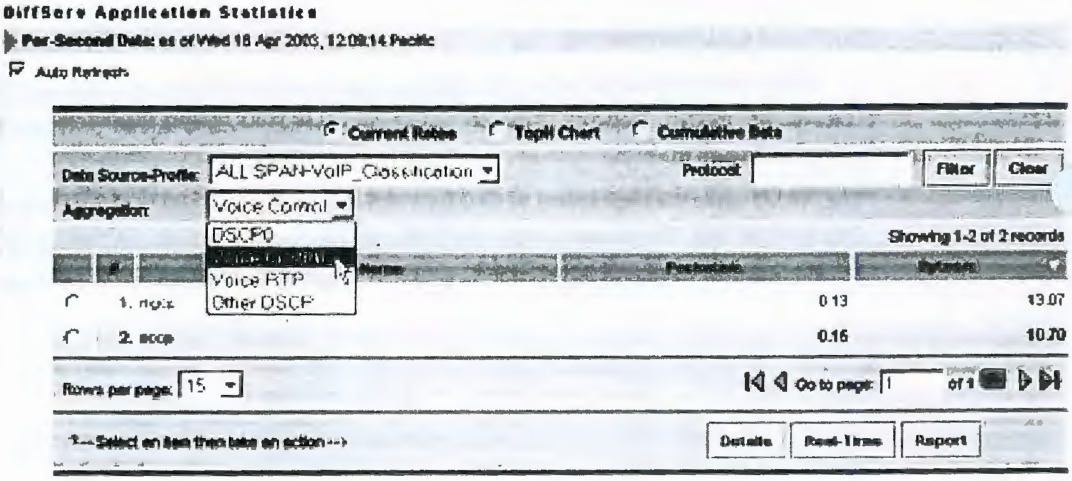
Catalyst 6k NAM - Active Call Detail

Current Data: as of Tue Jun 11 18:08:48 2002

SCCP call detail

	Calling Party	Called Party
Number	1002	1006
IP Address	172.20.80.184	172.20.80.183
Call Reference	17086663	17086664
Owner	Bilbo Baggins	Frodo Baggins
Call State	Connect	Connect
RTP Port	28002	21784
Line Instance	1	1
Conference Id	0	0
Pass Thru Party Id	4958291	4958305
RTP Sampling Period	20	20
Payload Type	G.711 ulaw 64k	G.711 ulaw 64k
RTP PRE Value	178	178
Silence Sup	Off	Off
Max Frames per Pkt	28086	28086
G.723 Bit Rate	-	-
Start Time	Tue Jun 11, 2002 08:48:40 PM	
Packets Sent	781	458
Packets Received	777	450
Octets Sent	134332	78776
Octets Received	133644	78840
Packet Loss (%)	0.0000	0.0000
Jitter (msec)	0	0
Switch Port	2/30	-

Figure 7
QoS Monitoring Using DSMON



DiffServ Application Statistics

Per-Second Data: as of Wed 16 Apr 2003, 12:08:14 Pacific

☑ Auto Refresh

● Current Rates ○ TopN Chart ○ Cumulative Data

Data Source-Profile: ALL SPAN-VoIP_Classification

Protocol:

Aggregation: Voice Control

Showing 1-2 of 2 records

	#	Name	Packets/s	Bytes/s
○	1.	mgcp	0.13	13.07
○	2.	sccp	0.16	10.70

Rows per page: 15

Go to page: 1 of 1

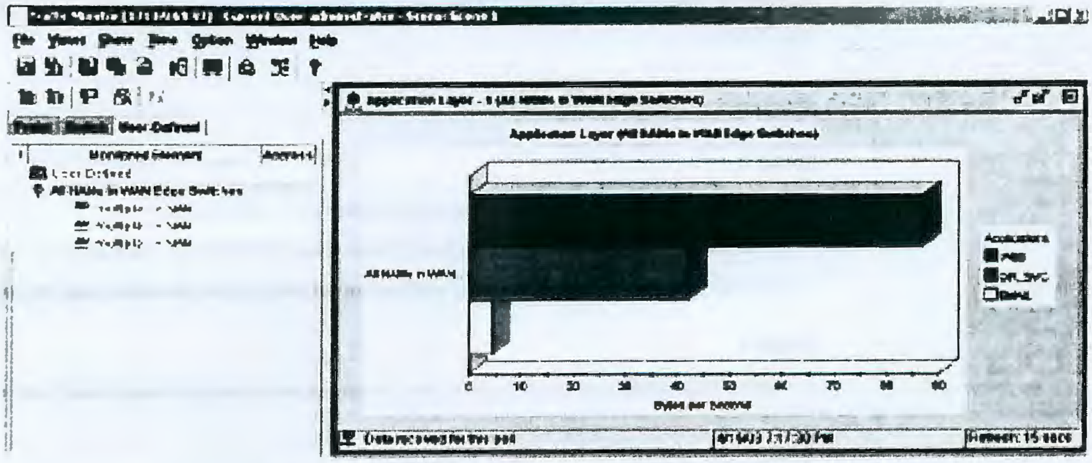
?-- Select an item then take an action -->

Capacity Planning and Other Extended Applications

The data from the NAMs across the network can be collected by NetScout nGenius Real-Time Monitor, a component of the CiscoWorks LAN Management Solution (LMS) to provide consolidated views of network traffic (Figure 8). The NAMs serve as data sources for several other standards-based applications for a variety of purposes including capacity planning, long-term historical reporting and trending, anomaly-based threat detection, etc.

Figure 8

Aggregating data from NAMs across the network using NetScout nGenius Real-Time Monitor


File Views Show Time Option Window Help
User Defined
All NAMs in WAN Edge Switches
Application Layer (All NAMs in WAN Edge Switches)
All NAMs in WAN
Applications
0
10
20
30
40
50
60
70
80
90
Bytes per Second
Refresh: 15 secs

Primary Advantages

- Integrated with network infrastructure—The NAMs occupy a single slot within the Cisco Catalyst 6500 Series or Cisco 7600 Series chassis and are deployed, managed, and supported as an integral part of the network infrastructure. They do not interfere with switching and routing functions and have their own processing resources. They are managed as a part of the network device using CiscoWorks management tools.
- Complete monitoring solution for LAN, WAN, and network-based services—The NAMs combine the functions of data collection agent and analysis application in one and provide comprehensive monitoring using a variety of data sources including RMON, RMON2 and NetFlow though the embedded Traffic Analyzer.
- Total cost of ownership savings—The integrated nature of the NAM solution saves costs in acquiring network device-specific features like mini-RMON, and in maintenance and technical support. The NAM Traffic Analyzer is embedded in the NAMs at no extra cost.
- Extensible, standards-based solution—The NAMs are compliant with open standards, and can be used with different monitoring applications to meet diverse needs.
- Secure solution—The NAM Traffic Analyzer can be deployed with up to 168-bit encryption, and SNMP can be disabled for fortifying external access to the NAM. The NAMs support Secure Shell (SSH) for secured command-line access.

Network Monitoring Solutions

Cisco Systems offers a wide variety of solutions to provide complete visibility into network infrastructure. The comprehensive Cisco solution includes embedded technologies such as mini-RMON, NetFlow, Service Assurance Agent (SAA), Network-Based Application Recognition (NBAR); NAMs for the Cisco Catalyst 6500 Series and Cisco 7600 Series for value-added traffic analysis. and CiscoWorks network monitoring applications. nGenius Real-Time Monitor, a component of the CiscoWorks LAN Management Solution (LMS), collects mini-RMON data from switches to provide port utilization statistics and uses data from NAMs across the network to provide broad-based analysis and reports on network traffic. Cisco AVVID (Architecture for Voice, Video and Integrated Data) partners extend the Cisco network monitoring solution through a variety of applications that use embedded data sources and NAMs.

Technical Specifications

NAM-1

- High-performance dual processor architecture, 512 MB RAM
- Two data collection interfaces to backplane: 1 for SPAN/VACL data sources, 1 for NetFlow
- Second generation fabric enabled platform with interface to both bus and crossbar based architectures

NAM-2

- Extra high-performance dual processor architecture with hardware-based packet acceleration, 1 GB RAM
- Gigabit monitoring performance
- Three data collection interfaces to backplane: 2 for SPAN/VACL data sources (can be used independently or together), 1 for NetFlow
- Second generation fabric enabled platform with interface to both bus and crossbar based architectures

Supported Platforms

- NAM-1 and NAM-2 can be deployed in any slot in Cisco Catalyst 6500 and 6000 Series switches and Cisco 7600 Series routers [both bus- and crossbar (fabric)-based architectures]; multiple NAMs can be placed in the same chassis
- Supported with Cisco IOS® Software or Cisco Catalyst Operating System on the Supervisor Engine

Supported Topologies and Data Sources

- LAN—Switch Port Analyzer (SPAN) or Remote SPAN (RSPAN), VLAN ACL(VACL)-based captures, NetFlow (v1, v5, v6, v7, v8)
- WAN—NetFlow (v1, v5, v6, v7, v8) from local and remote devices, VLAN ACL (VACL)-based captures for FlexWAN/Optical Service Module (OSM) interfaces (Cisco IOS Software only)

Supported Interfaces and Applications

- HTTP/HTTPS with embedded web based NAM Traffic Analyzer
- SNMP v1, v2 with NetScout nGenius Real Time Monitor and other standards based applications

NAM Traffic Analyzer

- Embedded in NAM Software Version 2.2 and later for NAM-1/NAM-2
- Web based—Requires Microsoft Internet Explorer 5.0 or Netscape 4.7 (minimum)
- Supports Secure Sockets Layer (SSL) security with up to 168-bit encryption
- Role-based user authorization and authentication locally or using TACACS+
- Real-time and historical statistics (up to 100 days) on LAN/WAN traffic and network-based services

NAM Software Version 3.1

- Supports NAM-1 (part number WS-SVC-NAM-1), NAM-2 (WS-SVC-NAM-2) and first-generation NAM (WS-X6380-NAM)
- Supported with Cisco IOS® Software Release 12.1(13)E or Cisco Catalyst Operating System 7.3(1) minimum on the Supervisor Engine

Supported MIB Groups

The NAMs are standards-compliant and support RMON and RMON2 MIBs, as well as several extensions. The major MIB groups supported in the NAMs are:

- MIB-II (RFC 1213)—All groups except Exterior Gateway Protocol (EGP) and transmission
- RMON (RFC 2819)—All groups
- RMON2 (RFC2021)—All groups
- SMON (RFC2613)—DataSourceCaps and smonStats
- DSMON (RFC 3287)
- HC-RMON (RFC 3273)
- Application Response Time (ART)

Supported Protocols

The NAMs provide RMON2 statistics on several-hundred unique protocols, including those defined in RFC 2896, and several Cisco proprietary protocols. In addition, the NAMs can automatically detect unknown protocols and users have the flexibility to customize the protocol directory.

Examples of Protocols Supported by the NAMs for RMON2 Statistics:

- TCP and UDP over IP including IPv6
- VoIP including SCCP(Skinny), RTP/RTCP, MGCP, SIP
- Mobile IP protocols (Both IP in IP and GRE tunnelling)
- Storage area network (SAN) protocols including Fiber Channel over TCP/IP
- AppleTalk, DECnet, Novell, Microsoft
- Database protocols including Oracle, Sybase
- Bridge and router protocols
- Cisco proprietary protocols
- Unknown protocols by TCP/UDP ports, RPC program numbers, etc.

Physical Specifications

- Dimensions (H x W x D): 1.2 x 14.4 x 16 in. (3.0 x 35.6 x 40.6 cm); Occupies any 1 slot in the chassis

Operating Environment

- Operating temperature: 32 F (0 C) to 104 F (40 C)
- Nonoperating and storage temperature: -40 F (-40 C) to 158 F (70 C)
- Operating relative humidity: 10% to 90% (noncondensing)
- Nonoperating relative humidity: 5% to 95% (noncondensing)
- Operating and nonoperating altitude: Sea level to 10,000 ft (3050 m)

Agency Approvals

- Regulatory: CE Marking (89/366/EEC and 73/23/EEC)
- Safety: UL 1950, CAN/CSA-C22.2 No. 950, EN 60950, IEC 60950
- Electromagnetic Emissions: FCC Part 15 (CFR 47) Class A, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55024, EN50082-1

Ordering Information

Cisco Part Number	Description
WS-SVC-NAM-1	Network Analysis Module-1 for Cisco Catalyst 6500 Series and Cisco 7600 Series
WS-SVC-NAM-2	Network Analysis Module-2 for Cisco Catalyst 6500 Series and Cisco 7600 Series
SC-SVC-NAM-3.1	Network Analysis Module Software v 3.1 for NAM-1, NAM-2 (includes ART, VoIP)

- The use of mini-RMON in Cisco Catalyst 6500 Series and Cisco 7600 Series with NAMs installed does not require the purchase of a separate RMON agent license.
- The Application Response Time (ART) MIB and the VoIP monitoring features are included at no extra cost for the NAM-1 and NAM-2. They require purchase of separate licenses (SC6K-NAM-ART-LIC= and SC6K-NAM-VOIP-LIC=) with the first-generation NAM (WS-X6380-NAM)
- Service Part Numbers for NAM-1 and NAM-2 are CON-xxx-WSSVCNAM1 and CON-xxx-WSSVNAM2 respectively, where "xxx" stands for level of support (for example, xxx= SNT = 8x5x Next Business Day)

More Information

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice FB

CHAPTER 32

Configuring PFC QoS

This chapter describes how to configure quality of service (QoS) as implemented on the policy feature card (PFC) on the Catalyst 6500 series switches.

Note For complete syntax and usage information for the commands used in this publication, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter contains these sections:

- Understanding How PFC QoS Works, page 32-1
- PFC QoS Default Configuration, page 32-24
- PFC QoS Configuration Guidelines and Restrictions, page 32-29
- Configuring PFC QoS, page 32-31

Note

- With Release 12.1(13)E and later releases and with an MSFC2, you can configure Network-Based Application Recognition (NBAR) on LAN ports instead of using PFC QoS.
- All ingress and egress traffic on a port that is configured with NBAR is processed in software on the MSFC2.
- The PFC2 provides hardware support for input ACLs on ports where you configure NBAR.
- When PFC QoS is enabled, the traffic through ports where you configure NBAR passes through the ingress and egress queues and drop thresholds. When PFC QoS is enabled, the MSFC2 sets egress CoS equal to egress IP precedence.
- After passing through an ingress queue, all traffic is processed in software on the MSFC2 on ports where you configure NBAR.
- To configure NBAR, refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

Understanding How PFC QoS Works

Typically, networks operate on a *best-effort* delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

QoS selects network traffic (both unicast and multicast), prioritizes it according to its relative importance, and uses congestion avoidance to provide priority-indexed treatment; QoS can also limit the bandwidth used by network traffic. QoS makes network performance more predictable and bandwidth utilization more effective.

Note On the Catalyst 6500 series switches, queue architecture and QoS queueing features such as Weighted-Round Robin (WRR) and Weighted Random Early Detection (WRED) are implemented with a fixed configuration in Application Specific Integrated Circuits (ASICs). The queueing architecture cannot be reconfigured. For more information, see the "Receive Queues" section on page 32-13 and the "Transmit Queues" section on page 32-21.

These sections describe PFC QoS:

- Hardware Supported by PFC QoS, page 32-2
- QoS Terminology, page 32-3
- PFC QoS Feature Flowcharts, page 32-5
- PFC QoS Feature Summary, page 32-11
- Ingress LAN Port Features, page 32-12
- PFC Marking and Policing, page 32-16
- LAN Egress Port Features, page 32-21
- PFC QoS Statistics Data Export, page 32-24

Hardware Supported by PFC QoS

With Release 12.1(11a)E and later, PFC QoS supports both LAN ports and optical services module (OSM) ports:

- *LAN ports* are Ethernet ports on Ethernet switching modules, except for the 4-port Gigabit Ethernet WAN (GBIC) module (OSM-4GE-WAN). Except for the OSM-4GE-WAN module, OSMs have four Ethernet LAN ports in addition to WAN ports. With earlier releases, PFC QoS supports only LAN ports.
- *OSM ports* are the WAN ports on OSMs. The PFC provides ingress QoS for traffic from OSM ports. For more information, see the following sections:
  - "Ingress OSM Port Features" section on page 32-11
  - "Egress OSM Port Features" section on page 32-12
  - "PFC Marking and Policing" section on page 32-16
  - "Attaching Policy Maps" section on page 32-21
  - "Configuring the Trust State of Ethernet LAN and OSM Ingress Ports" section on page 32-51
- Refer to the following publication for information about additional OSM QoS features:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm
- The PFC does not provide QoS for FlexWAN module ports. Refer to the following publications for information about FlexWAN module QoS features:
  - *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.1:

    http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/index.htm

- *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.1:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_r/index.htm

- *Class-Based Marking*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/cbpmark2.htm

- *Traffic Policing*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtpoli.htm

- *Distributed Class-Based Weighted Fair Queueing and Distributed Weighted Random Early Detection*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtcbwred.htm

- *Distributed Low Latency Queueing*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtllqvip.htm

- *Configuring Burst Size in Low Latency Queueing*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtcfgbst.htm

- *Distributed Traffic Shaping*:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdts.htm

- MPLS QoS:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/mpls.htm

QoS Terminology

This section defines some QoS terminology:

- *Packets* carry traffic at Layer 3.
- *Frames* carry traffic at Layer 2. Layer 2 frames carry Layer 3 packets.
- *Labels* are prioritization values carried in Layer 3 packets and Layer 2 frames:
  - Layer 2 class of service (CoS) values, which range between zero for low priority and seven for high priority:

    Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p CoS value in the three least significant bits.

    Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most significant bits, which are called the User Priority bits.

    Other frame types cannot carry Layer 2 CoS values.

Note On LAN ports configured as Layer 2 ISL trunks, all traffic is in ISL frames. On LAN ports configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

- Layer 3 IP precedence values—The IP version 4 specification defines the three most significant bits of the 1-byte Type of Service (ToS) field as IP precedence. IP precedence values range between zero for low priority and seven for high priority.
- Layer 3 differentiated services code point (DSCP) values—The Internet Engineering Task Force (IETF) has defined the six most significant bits of the 1-byte IP ToS field as the DSCP. The per-hop behavior represented by a particular DSCP value is configurable. DSCP values range between 0 and 63 (see the "Configuring DSCP Value Maps" section on page 32-64).

Note Layer 3 IP packets can carry either an IP precedence value or a DSCP value. PFC QoS supports the use of either value, since DSCP values are backwards compatible with IP precedence values (see Table 32-1 on page 32-4).

Table 32-1 IP Precedence and DSCP Values

3-bit IP Precedence	6 MSb[1] of ToS						6-bit DSCP	3-bit IP Precedence	6 MSb[1] of ToS						6-bit DSCP
	8	7	6	5	4	3			8	7	6	5	4	3	
0	0	0	0	0	0	0	0	4	1	0	0	0	0	0	32
	0	0	0	0	0	1	1		1	0	0	0	0	1	33
	0	0	0	0	1	0	2		1	0	0	0	1	0	34
	0	0	0	0	1	1	3		1	0	0	0	1	1	35
	0	0	0	1	0	0	4		1	0	0	1	0	0	36
	0	0	0	1	0	1	5		1	0	0	1	0	1	37
	0	0	0	1	1	0	6		1	0	0	1	1	0	38
	0	0	0	1	1	1	7		1	0	0	1	1	1	39
1	0	0	1	0	0	0	8	5	1	0	1	0	0	0	40
	0	0	1	0	0	1	9		1	0	1	0	0	1	41
	0	0	1	0	1	0	10		1	0	1	0	1	0	42
	0	0	1	0	1	1	11		1	0	1	0	1	1	43
	0	0	1	1	0	0	12		1	0	1	1	0	0	44
	0	0	1	1	0	1	13		1	0	1	1	0	1	45
	0	0	1	1	1	0	14		1	0	1	1	1	0	46
	0	0	1	1	1	1	15		1	0	1	1	1	1	47
2	0	1	0	0	0	0	16	6	1	1	0	0	0	0	48
	0	1	0	0	0	1	17		1	1	0	0	0	1	49
	0	1	0	0	1	0	18		1	1	0	0	1	0	50
	0	1	0	0	1	1	19		1	1	0	0	1	1	51
	0	1	0	1	0	0	20		1	1	0	1	0	0	52
	0	1	0	1	0	1	21		1	1	0	1	0	1	53
	0	1	0	1	1	0	22		1	1	0	1	1	0	54
	0	1	0	1	1	1	23		1	1	0	1	1	1	55
3	0	1	1	0	0	0	24	7	1	1	1	0	0	0	56
	0	1	1	0	0	1	25		1	1	1	0	0	1	57
	0	1	1	0	1	0	26		1	1	1	0	1	0	58
	0	1	1	0	1	1	27		1	1	1	0	1	1	59
	0	1	1	1	0	0	28		1	1	1	1	0	0	60
	0	1	1	1	0	1	29		1	1	1	1	0	1	61
	0	1	1	1	1	0	30		1	1	1	1	1	0	62
	0	1	1	1	1	1	31		1	1	1	1	1	1	63

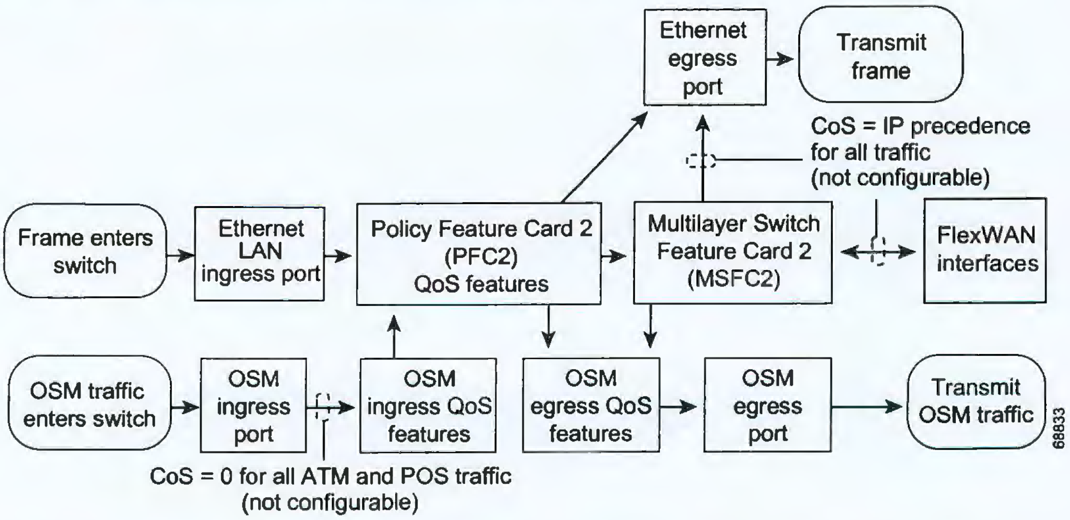
[1] MSb = most significant bit

- *Classification* is the selection of traffic to be marked.
- *Marking*, according to RFC 2475, is the process of setting a Layer 3 DSCP value in a packet; in this publication, the definition of marking is extended to include setting Layer 2 CoS values.
- *Scheduling* is the assignment of Layer 2 frames to a queue. PFC QoS assigns frames to a queue based on Layer 2 CoS values.
- *Congestion avoidance* is the process by which PFC QoS reserves ingress and egress LAN port capacity for Layer 2 frames with high-priority Layer 2 CoS values. PFC QoS implements congestion avoidance with Layer 2 CoS value-based drop thresholds. A drop threshold is the percentage of queue buffer utilization above which frames with a specified Layer 2 CoS value is dropped, leaving the buffer available for frames with higher-priority Layer 2 CoS values.
- *Policing* is limiting bandwidth used by a flow of traffic. Policing is done on the Policy Feature Card (PFC) or on the Policy Feature Card 2 (PFC2) and distributed forwarding cards (DFCs). Policing can mark or drop traffic.

PFC QoS Feature Flowcharts

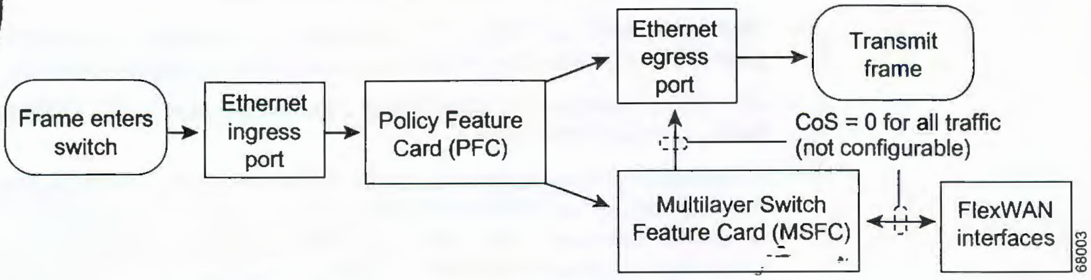
Figure 32-1 show how traffic flows through the components that support PFC QoS features.

Figure 32-1 Traffic Flow Through PFC QoS Features with PFC2


Ethernet egress port
Transmit frame
CoS = IP precedence for all traffic (not configurable)
Frame enters switch
Ethernet LAN ingress port
Policy Feature Card 2 (PFC2) QoS features
Multilayer Switch Feature Card 2 (MSFC2)
FlexWAN interfaces
OSM traffic enters switch
OSM ingress port
OSM ingress QoS features
OSM egress QoS features
OSM egress port
Transmit OSM traffic
68833
CoS = 0 for all ATM and POS traffic (not configurable)

Note PFC QoS supports traffic from OSMs with Release 12.1(11a)E and later.

Figure 32-2 Traffic Flow Through PFC QoS Features with PFC


Frame enters switch
Ethernet ingress port
Policy Feature Card (PFC)
Ethernet egress port
Transmit frame
CoS = 0 for all traffic (not configurable)
Multilayer Switch Feature Card (MSFC)
FlexWAN interfaces
68003

Note

- The PFC can provide Layer 3 switching for FlexWAN traffic but does not provide PFC QoS for FlexWAN traffic.
- PFC QoS does not change the ToS byte in FlexWAN ingress traffic.
- Traffic that is Layer 3-switched does not go through the MSFC and retains the Layer 2 CoS value assigned by the PFC.

Figure 32-3 through Figure 32-8 show how the PFC QoS features are implemented on the switch components.

Figure 32-3 Ingress LAN Port Layer 2 PFC QoS Features

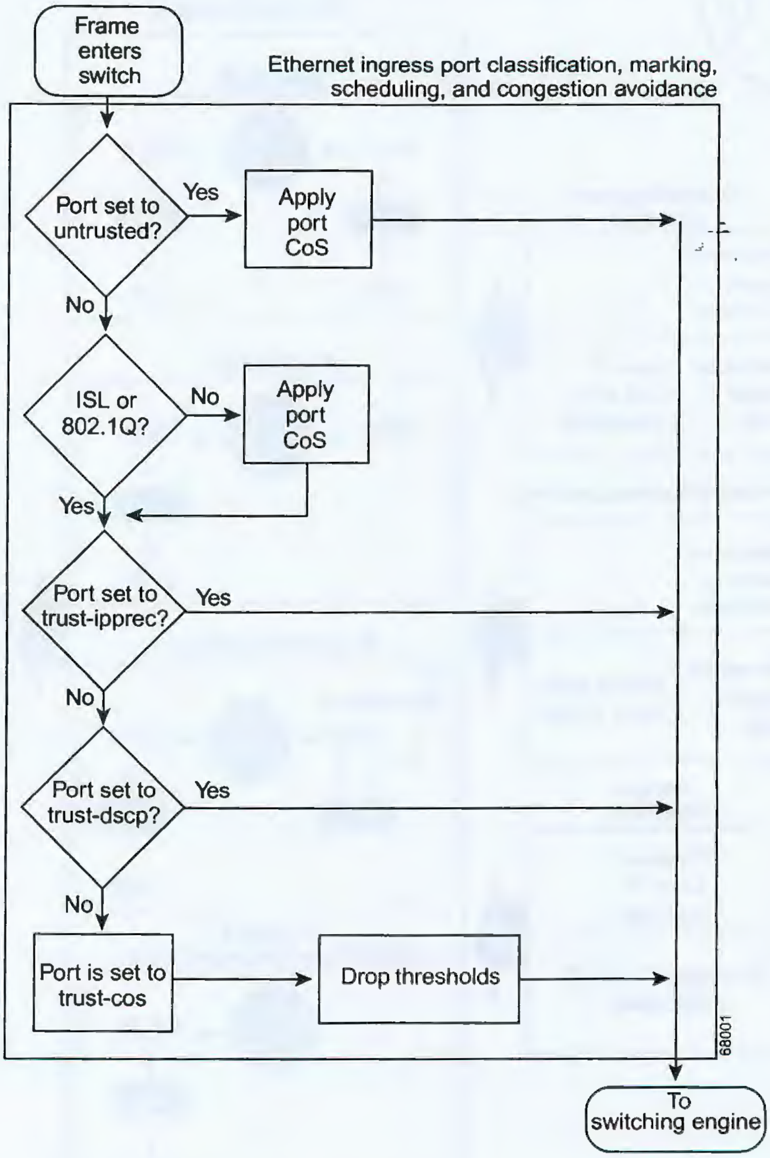


Figure 32-4 *PFC Classification, Marking, and Policing*

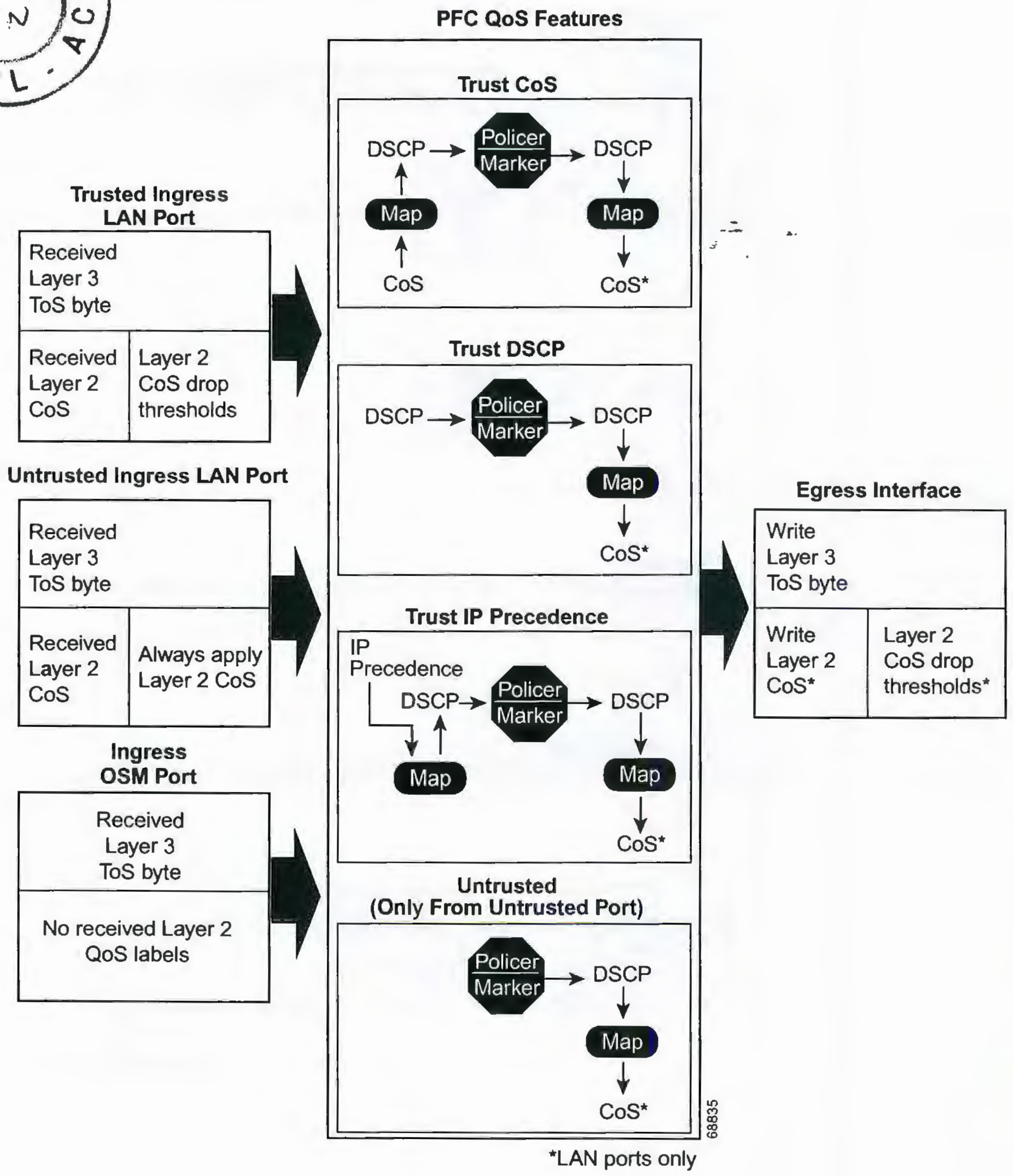


Figure 32-5 Marking with PFC2 and Multilayer Switch Feature Card 2

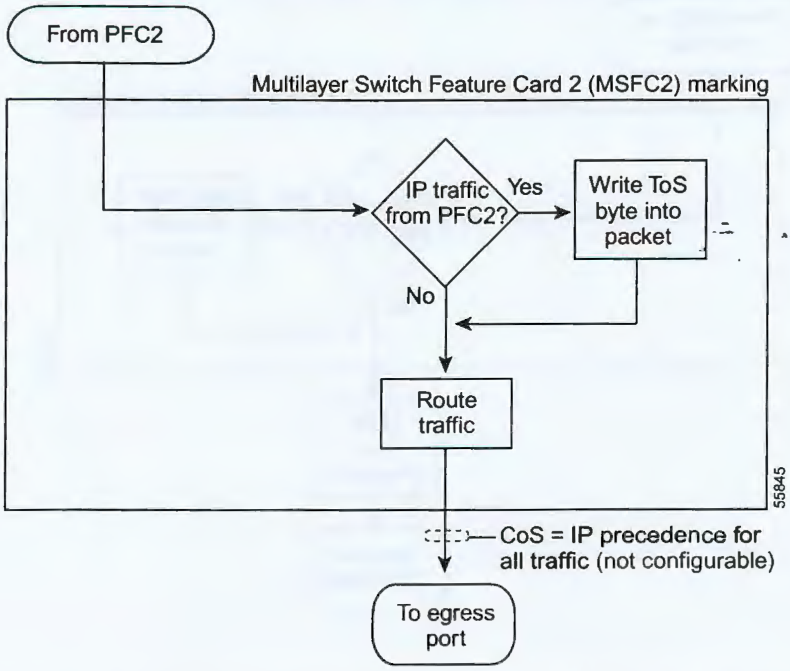

From PFC2
Multilayer Switch Feature Card 2 (MSFC2) marking
IP traffic from PFC2?
Yes
Write ToS byte into packet
No
Route traffic
55845
CoS = IP precedence for all traffic (not configurable)
To egress port

Figure 32-6 Marking with PFC1 and Multilayer Switch Feature Card 1 or 2

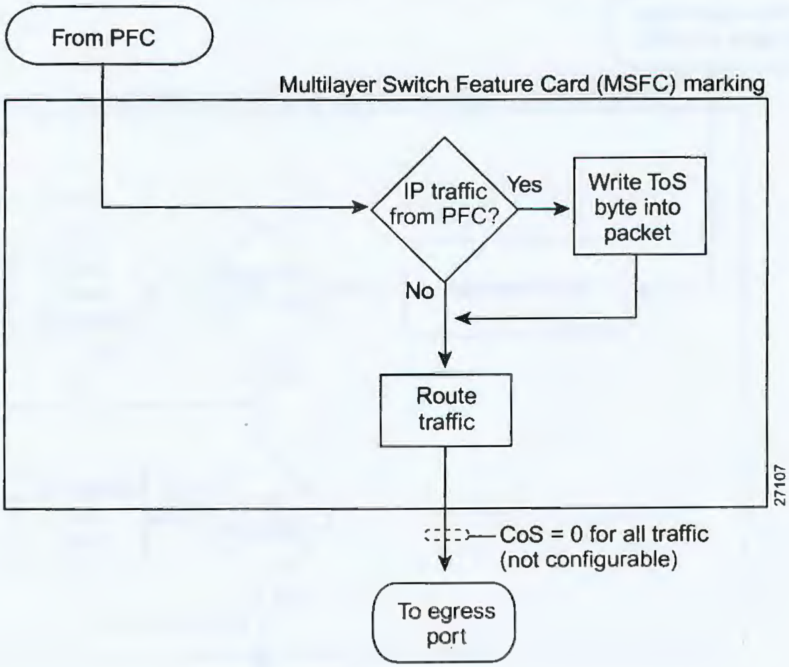

From PFC
Multilayer Switch Feature Card (MSFC) marking
IP traffic from PFC?
Yes
Write ToS byte into packet
No
Route traffic
27107
CoS = 0 for all traffic (not configurable)
To egress port

Figure 32-7 Egress WAN Port Marking

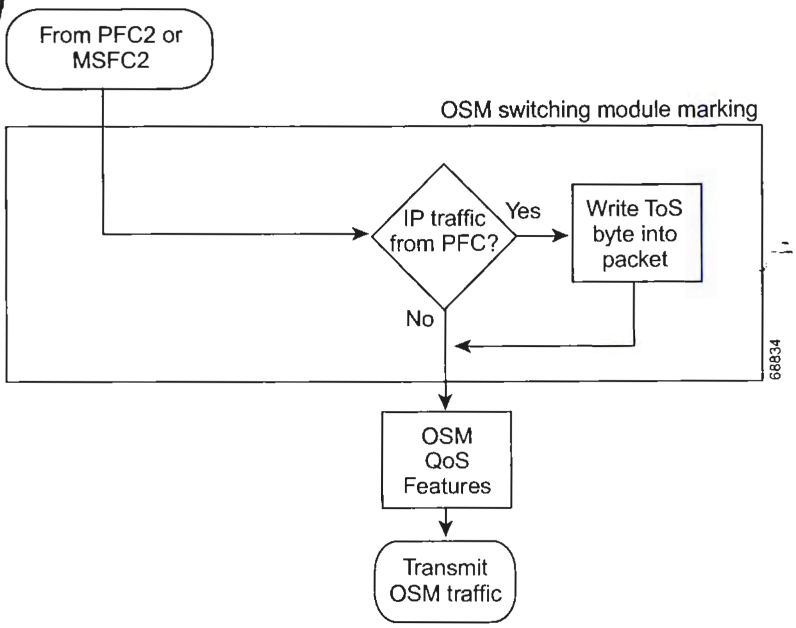
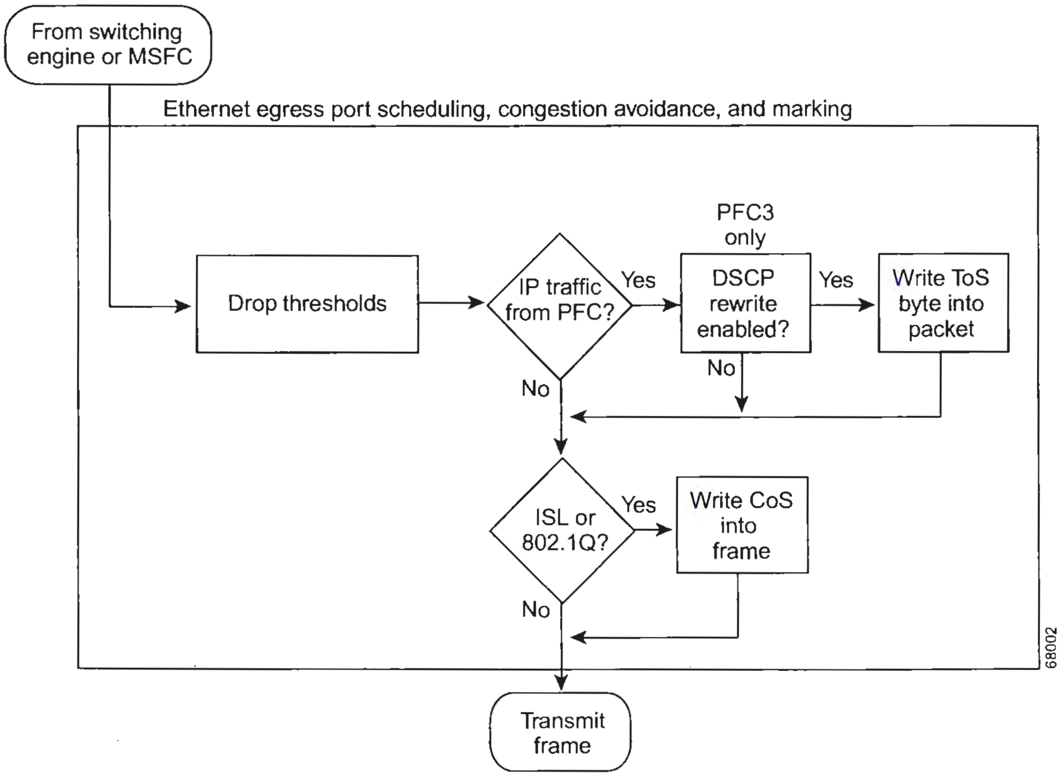


Figure 32-8 Egress LAN Port Scheduling, Congestion Avoidance, and Marking



PFC QoS Feature Summary

These sections summarize the PFC QoS features:

- Ingress LAN Port Features, page 32-11
- Ingress OSM Port Features, page 32-11
- PFC QoS Features, page 32-11
- Egress LAN Port Features, page 32-12
- Egress OSM Port Features, page 32-12
- MSFC Features, page 32-12

Ingress LAN Port Features

PFC QoS supports classification, marking, scheduling, and congestion avoidance using Layer 2 CoS values at ingress LAN ports. Classification, marking, scheduling, and congestion avoidance at ingress LAN ports do not use or set Layer 3 IP precedence or DSCP values. You can configure ingress LAN port trust states that can be used by the PFC to set Layer 3 IP precedence or DSCP values and the Layer 2 CoS value. See Figure 32-3 and the "Ingress LAN Port Features" section on page 32-12.

Ingress OSM Port Features

PFC QoS associates CoS zero with all traffic received through ingress OSM ports. You can configure ingress OSM port trust states that can be used by the PFC to set Layer 3 IP precedence or DSCP values and the Layer 2 CoS value. You can configure the trust state of each ingress OSM port as follows:

- Untrusted (default)
- Trust IP precedence
- Trust DSCP
- Trust CoS (CoS is always zero because the default port CoS is not configurable on OSM ports.)

PFC QoS Features

On the PFC, PFC QoS supports ingress classification, marking, and policing using policy maps. You can attach one policy map to an ingress port. Each policy map can contain multiple policy-map classes. You can configure a separate policy-map class for each type of traffic received through the ingress port. See the "PFC Marking and Policing" section on page 32-16.

Note

- You can globally disable marking and policing with the **mls qos queueing-only** command (see the Enabling Queueing-Only Mode, page 32-32).
- You can disable marking and policing on a per-interface basis with the **no mls qos** interface command (see the "Enabling or Disabling PFC Features on an Interface" section on page 32-49.

Egress LAN Port Features

PFC QoS supports egress LAN port scheduling and congestion avoidance using Layer 2 CoS values. Egress LAN port marking sets Layer 2 CoS values and Layer 3 DSCP values. See the "LAN Egress Port Features" section on page 32-21.

Egress OSM Port Features

Ingress PFC QoS sets Layer 3 DSCP values that can be used by the OSM egress QoS features.

MSFC Features

PFC QoS marks IP traffic transmitted to the MSFC with rewritten Layer 3 DSCP values. With PFC2, CoS is equal to IP precedence in all traffic sent from the MSFC2 to egress ports; with PFC1, CoS is zero.

Note Traffic that is Layer 3 switched does not go through the MFSC and retains the CoS value assigned by the PFC.

Ingress LAN Port Features

These sections describe ingress LAN port PFC QoS features:

- Ingress LAN Port Trust States, page 32-12
- Marking at Untrusted Ingress LAN Ports, page 32-13
- Marking at Trusted Ingress LAN Ports, page 32-13
- Ingress LAN Port Scheduling and Congestion Avoidance, page 32-13

Ingress LAN Port Trust States

The trust state of an ingress LAN port determines how the port marks, schedules, and classifies received Layer 2 frames, and whether or not congestion avoidance is implemented. You can configure the trust state of each ingress LAN port as follows:

- Untrusted (default)
- Trust IP precedence (not supported on **1q4t** LAN ports except Gigabit Ethernet)
- Trust DSCP (not supported on **1q4t** LAN ports except Gigabit Ethernet)
- Trust CoS (not supported on **1q4t** LAN ports except Gigabit Ethernet)

See the "Configuring the Trust State of Ethernet LAN and OSM Ingress Ports" section on page 32-51. PFC QoS implements ingress LAN port congestion avoidance only on LAN ports configured to trust CoS.

Note Ingress LAN port marking, scheduling, and congestion avoidance use Layer 2 CoS values and does not use or set Layer 3 IP precedence or DSCP values.

Marking at Untrusted Ingress LAN Ports

PFC QoS marks all frames received through untrusted ingress LAN ports with the ingress port CoS value (the default is zero). PFC QoS does not implement ingress port congestion avoidance on untrusted ingress LAN ports.

Marking at Trusted Ingress LAN Ports

When an ISL frame enters the Catalyst 6500 series switch through a trusted ingress LAN port, PFC QoS accepts the three least significant bits in the User field as a CoS value. When an 802.1Q frame enters the switch through a trusted ingress LAN port, PFC QoS accepts the User Priority bits as a CoS value. PFC QoS marks all traffic received in untagged frames with the ingress port CoS value.

Note The ingress port CoS value is configurable for each ingress LAN port (see the "Configuring the Ingress LAN Port CoS Value" section on page 32-52).

Ingress LAN Port Scheduling and Congestion Avoidance

On ingress LAN ports configured to trust CoS, PFC QoS uses Layer 2 CoS-value based receive-queue drop thresholds to avoid congestion (see the "Configuring the Trust State of Ethernet LAN and OSM Ingress Ports" section on page 32-51).

Receive Queues

Enter the **show queueing interface {ethernet | fastethernet | gigabitethernet | tengigabitethernet}** *slot/port* **| include type** command to see the queue structure of a LAN port.

- **1q2t** indicates one standard queue with one configurable tail-drop threshold and one nonconfigurable tail-drop threshold.
- **1q4t** indicates one standard queue with four configurable tail-drop thresholds (usable only on Gigabit Ethernet ports).
- **1p1q4t** indicates one strict-priority queue and one standard queue with four configurable tail-drop thresholds.
- **1p1q0t** indicates one strict-priority queue and one standard queue with no configurable threshold (effectively a tail-drop threshold at 100 percent).
- **1p1q8t** indicates one strict-priority queue and one standard queue with eight configurable WRED-drop thresholds and one non-configurable (100 percent) tail-drop threshold.

Strict-priority queues are queues that are serviced in preference to other queues. PFC QoS services traffic in a strict-priority queue before servicing the standard queue. When PFC QoS services the standard queue, after receiving a packet, it checks for traffic in the strict-priority queue. If PFC QoS detects traffic in the strict-priority queue, it suspends its service of the standard queue and completes service of all traffic in the strict-priority queue before returning to the standard queue.

Scheduling

PFC QoS schedules traffic through the receive queues based on Layer 2 CoS values. In the **1p1q4t**, **1p1q0t** and **1p1q8t** default configurations, PFC QoS assigns all traffic with CoS 5 to the strict-priority queue; PFC QoS assigns all other traffic to the standard queue. In the **1q4t** default configuration, PFC QoS assigns all traffic to the standard queue.

Congestion Avoidance

If an ingress LAN port is configured to trust CoS, PFC QoS implements Layer 2 CoS-value-based receive-queue drop thresholds to avoid congestion in received traffic.

1q2t ingress LAN ports have this default drop-threshold configuration:

- Frames with CoS 0, 1, 2, 3, or 4 go to tail-drop threshold 1, where the switch drops incoming frames when the standard receive-queue buffer is 80 percent full.
- Frames with CoS 5, 6, or 7 go to tail-drop threshold 2, where the switch drops incoming frames when the standard receive-queue buffer is 100 percent full.

1q4t ingress LAN ports have this default drop-threshold configuration:

- Using receive-queue tail-drop threshold 1, the switch drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
- Using receive-queue tail-drop threshold 2, the switch drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
- Using receive-queue tail-drop threshold 3, the switch drops incoming frames with CoS 4 or 5 when the receive-queue buffer is 80 percent or more full.
- Using receive-queue tail-drop threshold 4, the switch drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.

1p1q4t ingress LAN ports have this default drop-threshold configuration:

- Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue.
  - Using standard receive-queue tail-drop threshold 1, the switch drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
  - Using standard receive-queue tail-drop threshold 2, the switch drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
  - Using standard receive-queue tail-drop threshold 3, the switch drops incoming frames with CoS 4 when the receive-queue buffer is 80 percent or more full.
  - Using standard receive-queue tail-drop threshold 4, the switch drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.

1p1q0t ingress LAN ports have this default drop-threshold configuration:

- Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue. The switch drops incoming frames when the receive-queue buffer is 100 percent full.

1p1q8t ports have this default drop-threshold configuration:

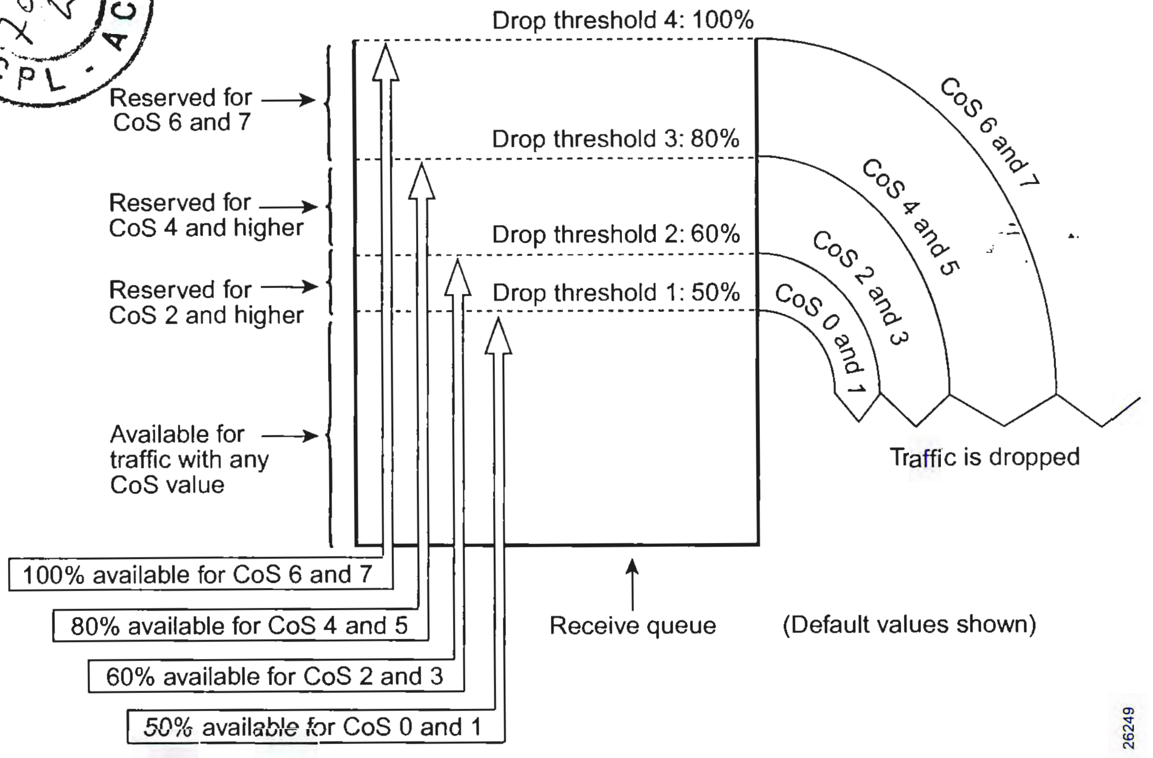
- Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the switch drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue, which uses WRED-drop thresholds:
  - Using standard receive-queue WRED-drop threshold 1 for incoming frames with CoS 0, the switch starts to drop frames when the receive-queue buffer is 40 percent full and drops all frames with CoS 0 when the receive-queue buffer is 70 percent or more full.
  - Using standard receive-queue WRED-drop threshold 2 for incoming frames with CoS 1, the switch starts to drop frames when the receive-queue buffer is 40 percent full and drops all frames with CoS 1 when the receive-queue buffer is 70 percent or more full.
  - Using standard receive-queue WRED-drop threshold 3 for incoming frames with CoS 2, the switch starts to drop frames when the receive-queue buffer is 50 percent full and drops all frames with CoS 2 when the receive-queue buffer is 80 percent or more full.
  - Using standard receive-queue WRED-drop threshold 4 for incoming frames with CoS 3, the switch starts to drop frames when the receive-queue buffer is 50 percent full and drops all frames with CoS 3 when the receive-queue buffer is 80 percent or more full.
  - Using standard receive-queue WRED-drop threshold 5 for incoming frames with CoS 4, the switch starts to drop frames when the receive-queue buffer is 60 percent full and drops all frames with CoS 4 when the receive-queue buffer is 90 percent or more full.
  - Using standard receive-queue WRED-drop threshold 6 for incoming frames with CoS 6, the switch starts to drop frames when the receive-queue buffer is 60 percent full and drops all frames with CoS 6 when the receive-queue buffer is 90 percent or more full.
  - Using standard receive-queue WRED-drop threshold 7 for incoming frames with CoS 7, the switch starts to drop frames when the receive-queue buffer is 70 percent full and drops all frames with CoS 7 when the receive-queue buffer is 100 percent or more full.

  Note You can configure the standard receive queue to use both a tail-drop and a WRED-drop threshold by mapping a CoS value to the queue or to the queue and a threshold. The switch uses the tail-drop threshold for traffic carrying CoS values mapped only to the queue. The switch uses WRED-drop thresholds for traffic carrying CoS values mapped to the queue and a threshold. See the "Configuring Standard Queue WRED-Drop Thresholds" section on page 32-55.

Note The explanations in this section use default values. You can configure many of the parameters (see the "Configuring PFC QoS" section on page 32-31). All LAN ports of the same type use the same drop-threshold configuration.

Figure 32-9 illustrates the drop thresholds for a **1q4t** ingress LAN port. Drop thresholds in other configurations function similarly.

Figure 32-9 Receive Queue Drop Thresholds


Drop threshold 4: 100%
Drop threshold 3: 80%
Drop threshold 2: 60%
Drop threshold 1: 50%
Reserved for CoS 6 and 7
Reserved for CoS 4 and higher
Reserved for CoS 2 and higher
Available for traffic with any CoS value
CoS 6 and 7
CoS 4 and 5
CoS 2 and 3
CoS 0 and 1
Traffic is dropped
100% available for CoS 6 and 7
80% available for CoS 4 and 5
60% available for CoS 2 and 3
50% available for CoS 0 and 1
Receive queue
(Default values shown)
26249

PFC Marking and Policing

Note

- To mark untrusted traffic without policing in Release 12.1(12c)E1 and later releases, use the **set ip dscp** or **set ip precedence** policy map class commands (see the "Configuring Policy Map Class Actions" section on page 32-42).
- To mark untrusted traffic without policing in earlier releases, create a policer that only marks and does not police.

These sections describe PFC marking and policing:

- Internal DSCP Values, page 32-17
- Policy Maps, page 32-18
- Policers, page 32-19
- Attaching Policy Maps, page 32-21
- Egress CoS and ToS Values, page 32-21

Note Filtering for PFC QoS can use Layer 2, 3, and 4 values. Marking uses Layer 2 CoS values and Layer 3 IP precedence or DSCP values.

Internal DSCP Values

These sections describe the internal DSCP values:

- Internal DSCP Sources, page 32-17
- Egress DSCP and CoS Sources, page 32-17

Internal DSCP Sources

During processing, PFC QoS represents the priority of all traffic (including non-IP traffic) with an internal DSCP value. PFC QoS derives the internal DSCP value from the following:

- For trust-cos traffic, from received or ingress port Layer 2 CoS values

Note Traffic from an untrusted ingress LAN port has the ingress port CoS value and if traffic from an untrusted ingress Ethernet port matches a trust-cos policer, PFC QoS derives the internal DSCP value from the ingress port CoS value.

- For trust-ipprec traffic, from received IP precedence values
- For trust-dscp traffic, from received DSCP values
- For untrusted traffic, from ingress port CoS or configured DSCP values

The trust state of traffic is the trust state of the ingress LAN port unless set otherwise by a matching ACE.

Note A **trust-cos** policer cannot restore received CoS in traffic from untrusted ingress LAN ports. Traffic from untrusted ingress LAN ports always has the ingress port CoS value.

PFC QoS uses configurable mapping tables to derive the internal 6-bit DSCP value from CoS or IP precedence, which are 3-bit values (see the"Mapping Received CoS Values to Internal DSCP Values" section on page 32-64 or the "Mapping Received IP Precedence Values to Internal DSCP Values" section on page 32-65).

Egress DSCP and CoS Sources

For egress IP traffic, PFC QoS creates a ToS byte from the internal DSCP value and sends it to the egress port to be written into IP packets. For **trust-dscp** and **untrusted** IP traffic, the ToS byte includes the original 2 least-significant bits from the received ToS byte.

Note The internal DSCP value can mimic an IP precedence value (see Table 32-1 on page 32-4).

For all egress traffic, PFC QoS uses a configurable mapping table to derive a CoS value from the internal DSCP value associated with traffic (see the "Mapping Internal DSCP Values to Egress CoS Values" section on page 32-65). PFC QoS sends the CoS value to the egress LAN ports for use in scheduling and to be written into ISL and 802.1Q frames.

Policy Maps

Note

- You can globally disable marking and policing with the **mls qos queueing-only** command (see the Enabling Queueing-Only Mode, page 32-32).
- You can disable marking and policing on a per-interface basis with the **no mls qos** interface command (see the "Enabling or Disabling PFC Features on an Interface" section on page 32-49.

The PFC supports filtering, marking, and policing using policy maps (see the "Configuring a Policy Map" section on page 32-40). Each policy map can contain multiple policy-map classes. You can configure a separate policy-map class for each type of received traffic.

Policy-map classes specify filtering with the following:

- Cisco IOS access control lists (optional for IP, required for IPX and MAC-Layer filtering)
- Class-map **match** commands for Layer 3 IP precedence and DSCP values

Policy-map classes specify actions with the following:

- (Optional) Policy-map class **trust** commands. If specified, PFC QoS applies the policy-map class trust state to matched traffic. Policy-map class trust states supersede ingress LAN port trust states.

  Note If traffic matches a policy-map class that does not contain a **trust** command, the trust state remains as set on the ingress LAN port.

- (Optional) Aggregate and microflow policers, which can use bandwidth limits to either mark or drop both conforming and nonconforming traffic. See the "PFC Marking and Policing" section on page 32-16.

The PFC uses the trust state (set by the ingress LAN port configuration or by a **trust** policy-map class command) to select the Layer 2 and Layer 3 PFC QoS labels that the egress port writes into the packets and frames before it is transmitted:

- Trust IP precedence—Sets the internal DSCP value to a mapped value based on received IP precedence (see the "Mapping Received IP Precedence Values to Internal DSCP Values" section on page 32-65).
- Trust DSCP—Sets the internal DSCP value to the received DSCP value.
- Trust CoS—Sets the internal DSCP value to a mapped value based on received or port CoS. With trust CoS, note the following:
  - Received CoS is overwritten with port CoS in traffic received through ports not configured to trust CoS.
  - Received CoS is preserved only in traffic received through ports configured to trust CoS.
  - Port CoS is applied to all traffic received in untagged frames, regardless of the port trust state.
  - For information about mapping, see the "Mapping Received CoS Values to Internal DSCP Values" section on page 32-64.
- Untrusted—Sets the internal DSCP value to a configured DSCP value.

  Note With the default values, PFC QoS applies DSCP zero to traffic from ingress LAN ports configured as untrusted.

Policers

Note Policing with the **conform-action transmit** keywords supersedes the ingress LAN port trust state of matched traffic with trust DSCP or with the trust state defined by a **trust** policy-map class command (see the "Configuring the Policy Map Class Trust State" section on page 32-43).

You can create policers that do the following:

- Mark traffic
- Limit bandwidth utilization and mark traffic

  For more information, see the "Creating Named Aggregate Policers" section on page 32-33 and the "Configuring Policy Map Class Actions" section on page 32-42.

Policing rates are based on the Layer 3 packet size. You specify the bandwidth utilization limit as a committed information rate (CIR). With a PFC2, you can also specify a higher peak information rate (PIR). Packets that exceed a rate are "out of profile" or "nonconforming."

In each policer, you specify if out-of-profile packets are to be dropped or to have a new DSCP value applied to them (applying a new DSCP value is called "markdown"). Because out-of-profile packets do not retain their original priority, they are not counted as part of the bandwidth consumed by in-profile packets.

With a PFC2, if you configure a PIR, the PIR out-of-profile action cannot be less severe than the CIR out-of-profile action. For example, if the CIR out-of-profile action is to mark down the traffic, then the PIR out-of-profile action cannot be to transmit the traffic.

For all policers, PFC QoS uses a configurable global table that maps the internal DSCP value to a marked-down DSCP value (see the "Configuring DSCP Markdown Values" section on page 32-66). When markdown occurs, PFC QoS gets the marked-down DSCP value from the table. You cannot specify marked-down DSCP values in individual policers.

Note By default, the markdown table is configured so that no markdown occurs: the marked-down DSCP values are equal to the original DSCP values. To enable markdown, configure the table appropriately for your network.

You can create two kinds of policers: *aggregate* and *microflow*:

- PFC QoS applies the bandwidth limits specified in an aggregate policer cumulatively to all flows in matched traffic. You can create up to 1023 aggregate policers. You can create two types of aggregate policer: named and per port. Both types can be attached to more than one port:
  - You define per-interface aggregate policers in a policy map class with the **police** command. If you attach a per-interface aggregate policer to multiple ingress ports, it polices the matched traffic on each ingress port separately.
  - You create named aggregate policers with the **mls qos aggregate-policer** command. If you attach a named aggregate policer to multiple ingress ports, it polices the matched traffic from all the ingress ports to which it is attached.

Note Aggregate policing works independently on each DFC-equipped switching module and independently on the PFC2, which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate policing statistics for each DFC-equipped switching module and for the PFC2 and any non-DFC-equipped switching modules supported by the PFC2.

- PFC QoS applies the bandwidth limit specified in a microflow policer separately to each flow in matched traffic as follows:
  - You can create microflow policers with up to 63 different rate and burst parameter combinations.
  - You create microflow policers in a policy map class with the **police flow** command.
  - For IPX microflow policing, PFC QoS considers IPX traffic with the same source network, destination network, and destination node to be part of the same flow, including traffic with different source nodes or source sockets.
  - For MAC-Layer microflow policing, PFC QoS considers MAC-Layer traffic with the same protocol and the same source and destination MAC-Layer addresses to be part of the same flow, including traffic with different ethertypes.
  - By default, microflow policers only affect traffic routed by the MSFC. To enable microflow policing of other traffic, including traffic in bridge groups, enter the **mls qos bridged** command (see the "Enabling Microflow Policing of Bridged Traffic" section on page 32-48).

You can include both an aggregate policer and a microflow policer in each policy map class to police a flow based on both its own bandwidth utilization and on its bandwidth utilization combined with that of other flows.

Note If traffic is both aggregate and microflow policed, then the aggregate and microflow policers must both be in the same policy-map class and each must use the same **conform-action** keyword option: **drop**, **set-dscp-transmit**, **set-prec-transmit**, or **transmit**.

For example, you could create a microflow policer with a bandwidth limit suitable for individuals in a group and you could create a named aggregate policer with bandwidth limits suitable for the group as a whole. You could include both policers in policy map classes that match the group's traffic. The combination would affect individual flows separately and the group aggregately.

For policy map classes that include both an aggregate and a microflow policer, PFC QoS responds to an out-of-profile status from either policer and, as specified by the policer, applies a new DSCP value or drops the packet. If both policers return an out-of-profile status, then if either policer specifies that the packet is to be dropped, it is dropped; otherwise PFC QoS applies a marked-down DSCP value.

Note To avoid inconsistent results, ensure that all traffic policed by the same aggregate policer has the same trust state.

Attaching Policy Maps

You can configure each ingress LAN port for either physical port-based PFC QoS (default) or VLAN-based PFC QoS (see the "Enabling VLAN-Based PFC QoS on Layer 2 LAN Ports" section on page 32-50) and attach a policy map to the selected port (see the "Attaching a Policy Map to an Interface" section on page 32-47).

On ports configured for port-based PFC QoS, you can attach a policy map to the ingress LAN port as follows:

- On a nontrunk ingress LAN port configured for port-based PFC QoS, all traffic received through the port is classified, marked, and policed according to the policy map attached to the port.
- On a trunking ingress LAN port configured for port-based PFC QoS, traffic in *all VLANs* received through the port is classified, marked, and policed according to the policy map attached to the port.

On a nontrunk ingress LAN port configured for VLAN-based PFC QoS, traffic received through the port is classified, marked, and policed according to the policy map attached to the *port's* VLAN.

On a trunking ingress LAN port configured for VLAN-based PFC QoS, traffic received through the port is classified, marked, and policed according to the policy map attached to the *traffic's* VLAN.

You can attach policy maps to OSM ports.

Egress CoS and ToS Values

PFC QoS associates CoS and ToS values with traffic as specified by the trust state and policers in the policy map (see the "Internal DSCP Values" section on page 32-17). The associated CoS and ToS are used at the egress port (see the "LAN Egress Port Features" section on page 32-21).

LAN Egress Port Features

These sections describe how PFC QoS schedules traffic through the transmit queues based on CoS values and uses CoS-value-based transmit-queue drop thresholds to avoid congestion in traffic transmitted from egress LAN ports:

- Transmit Queues, page 32-21
- Scheduling and Congestion Avoidance, page 32-22
- Marking, page 32-24

Note Egress LAN port scheduling and congestion avoidance uses Layer 2 CoS values. Egress LAN port marking writes Layer 2 CoS values into trunk traffic and the Layer 3 ToS byte into all IP traffic.

Transmit Queues

Enter the **show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** command to see the queue structure of an egress LAN port.

The command displays one of the following:

- **2q2t** indicates two standard queues, each with two configurable tail-drop thresholds
- **1p2q2t** indicates one strict-priority queue and two standard queues, each with two configurable WRED-drop thresholds.

- **1p3q1t** indicates one strict-priority queue and three standard queues, each with one configurable WRED-drop threshold (on **1p3q1t** ports, each standard queue also has one nonconfigurable tail-drop threshold).
- **1p2q1t** indicates one strict-priority queue and two standard queues, each with one configurable WRED-drop threshold (on **1p2q1t** ports, each standard queue also has one nonconfigurable tail-drop threshold).

All port types have a low-priority and a high-priority standard transmit queue. **1p3q1t** ports have a medium-priority standard transmit queue. **1p2q2t, 1p3q1t** and **1p2q1t** ports have a strict-priority transmit queue in addition to the standard queues.

On **2q2t** ports, the default PFC QoS configuration allocates a minimum of 80 percent of the total transmit queue size to the low-priority standard queue and a minimum of 20 percent to the high-priority standard queue.

On **1p2q2t, 1p3q1t,** and **1p2q1t** ports, the switch services traffic in the strict-priority queue before servicing the standard queues. When the switch is servicing a standard queue, after transmitting a packet, it checks for traffic in the strict-priority queue. If the switch detects traffic in the strict-priority queue, it suspends its service of the standard queue and completes service of all traffic in the strict-priority queue before returning to the standard queue.

On **1p2q2t** ports, the default PFC QoS configuration allocates a minimum of 70 percent of the total transmit queue size to the low-priority standard queue, a minimum of 15 percent to the high-priority standard queue, and a minimum of 15 percent to the strict-priority queue.

On **1p3q1t** ports, the transmit queue size is not configurable and is allocated equally among all queues.

On **1p2q1t** ports, the default PFC QoS configuration allocates a minimum of 50 percent of the total transmit queue size to the low-priority standard queue, a minimum of 30 percent to the high-priority standard queue, and a minimum of 20 percent to the strict-priority queue.

Note Transmit-queue size is limited to the configured value (see the "Setting the Receive-Queue Size Ratio on a 1p1q0t or 1p1q8t Ingress LAN Ports" section on page 32-62), but any queue can use all available bandwidth (bandwidth is only available when there is no traffic in the other queues).

Scheduling and Congestion Avoidance

These sections describe scheduling and congestion avoidance:

- 2q2t Ports, page 32-23
- 1p2q2t Ports, page 32-23
- 1p3q1t Ports, page 32-23
- 1p2q1t Ports, page 32-24

Note The explanations in these sections use default values. You can configure many of the parameters (for more information, see the "Configuring PFC QoS" section on page 32-31). All ports of the same type use the same drop-threshold configuration.

2q2t Ports

For **2q2t** ports, each transmit queue has two tail-drop thresholds that function as follows:

- Frames with CoS 0, 1, 2, or 3 go to the low-priority transmit queue (queue 1):
  - Using transmit queue 1, tail-drop threshold 1, the switch drops frames with CoS 0 or 1 when the low-priority transmit-queue buffer is 80 percent full.
  - Using transmit queue 1, tail-drop threshold 2, the switch drops frames with CoS 2 or 3 when the low-priority transmit-queue buffer is 100 percent full.
- Frames with CoS 4, 5, 6, or 7 go to the high-priority transmit queue (queue 2):
  - Using transmit queue 2, tail-drop threshold 1, the switch drops frames with CoS 4 or 5 when the high-priority transmit-queue buffer is 80 percent full.
  - Using transmit queue 2, tail-drop threshold 2, the switch drops frames with CoS 6 or 7 when the high-priority transmit-queue buffer is 100 percent full.

1p2q2t Ports

1p2q2t ports have a strict-priority queue and two standard transmit queues. The two standard transmit queues each have two WRED-drop thresholds.

- Frames with CoS 5 go to the strict-priority transmit queue (queue 3), where the switch drops frames only when the buffer is 100 percent full.
- Frames with CoS 0, 1, 2, or 3 go to the low-priority standard transmit queue (queue 1):
  - Using standard transmit queue 1, WRED-drop threshold 1, the switch drops frames with CoS 0 or 1 when the low-priority transmit-queue buffer is 80 percent full.
  - Using standard transmit queue 1, WRED-drop threshold 2, the switch drops frames with CoS 2 or 3 when the low-priority transmit-queue buffer is 100 percent full.
- Frames with CoS 4, 6, or 7 go to the high-priority standard transmit queue (queue 2):
  - Using standard transmit queue 2, WRED-drop threshold 1, the switch drops frames with CoS 4 when the high-priority transmit-queue buffer is 80 percent full.
  - Using standard transmit queue 2, WRED-drop threshold 2, the switch drops frames with CoS 6 or 7 when the high-priority transmit-queue buffer is 100 percent full.

1p3q1t Ports

1p3q1t ports have a strict-priority queue and three standard transmit queues. The standard transmit queues each have one WRED-drop threshold and one nonconfigurable tail-drop threshold.

- Frames with CoS 5 go to the strict-priority transmit queue (queue 4), where the switch drops frames only when the buffer is 100 percent full.
- Frames with CoS 0 and 1 go to the low-priority standard transmit queue (queue 1).
- Frames with CoS 2, 3, or 4 go to the medium-priority standard transmit queue (queue 2).
- Frames with CoS 6 or 7 go to the high-priority standard transmit queue (queue 3).

Note You can configure each standard transmit queue to use both a non-configurable 100 percent tail-drop threshold and a configurable WRED-drop threshold (see the "Configuring Standard Queue WRED-Drop Thresholds" section on page 32-55).

1p2q1t Ports

1p2q1t ports have a strict-priority queue and two standard transmit queues. The standard transmit queues each have one WRED-drop threshold and one nonconfigurable tail-drop threshold.

- Frames with CoS 5 go to the strict-priority transmit queue (queue 3), where the switch drops frames only when the buffer is 100 percent full.
- The standard transmit queues have WRED-drop thresholds:
  - Frames with CoS 0, 1, 2, or 3 go to the low-priority transmit queue (queue 1), where the switch starts to drop frames when the low-priority transmit-queue buffer is 70 percent full and drops all frames with CoS 0, 1, 2, or 3 when the buffer is 100 percent full.
  - Frames with CoS 4, 6, or 7 go to the high-priority transmit queue (queue 2), where the switch starts to drop frames when the high-priority transmit-queue buffer is 70 percent full and drops all frames with CoS 4, 6, or 7 when the buffer is 100 percent full.

Note You can configure each standard transmit queue to use both the tail-drop and the WRED-drop threshold. See the "Configuring Standard Queue WRED-Drop Thresholds" section on page 32-55.

Marking

When traffic is transmitted from the switch, PFC QoS writes the ToS byte into IP packets. On LAN ports, PFC QoS also writes the CoS value that was used for scheduling and congestion avoidance into ISL and 802.1Q frames (see the "Egress CoS and ToS Values" section on page 32-21).

PFC QoS Statistics Data Export

Note Release 12.1(11b)E or later supports PFC QoS statistics data export.

The PFC QoS statistics data export feature generates per-LAN-port and per-aggregate policer utilization information and forwards this information in UDP packets to traffic monitoring, planning, or accounting applications. You can enable PFC QoS statistics data export on a per-LAN-port or on a per-aggregate policer basis. The statistics data generated per port consists of counts of the input and output packets and bytes. The aggregate policer statistics consist of counts of allowed packets and counts of packets exceeding the policed rate.

The PFC QoS statistics data collection occurs periodically at a fixed interval, but you can configure the interval at which the data is exported. PFC QoS statistics collection is enabled by default, and the data export feature is disabled by default for all ports and all aggregate policers configured on the Catalyst 6500 series switch.

Note The PFC QoS statistics data export feature is completely separate from NetFlow Data Export and does not interact with it.

PFC QoS Default Configuration

Table 32-2 shows the PFC QoS default configuration.

Table 32-2 PFC QoS Default Configuration

Feature	Default Value
PFC QoS global enable state	Disabled **Note** With PFC QoS enabled and all other PFC QoS parameters at default values, PFC QoS sets Layer 3 DSCP to zero and Layer 2 CoS to zero in all traffic transmitted from the switch.
PFC QoS queueing-only mode	Disabled
PFC QoS port enable state	Enabled when PFC QoS is globally enabled
Port CoS value	0
Microflow policing	Enabled
IntraVLAN microflow policing	Disabled
Port-based or VLAN-based PFC QoS	Port-based
CoS to DSCP map (DSCP set from CoS values)	CoS 0 = DSCP 0 CoS 1 = DSCP 8 CoS 2 = DSCP 16 CoS 3 = DSCP 24 CoS 4 = DSCP 32 CoS 5 = DSCP 40 CoS 6 = DSCP 48 CoS 7 = DSCP 56
IP precedence to DSCP map (DSCP set from IP precedence values)	IP precedence 0 = DSCP 0 IP precedence 1 = DSCP 8 IP precedence 2 = DSCP 16 IP precedence 3 = DSCP 24 IP precedence 4 = DSCP 32 IP precedence 5 = DSCP 40 IP precedence 6 = DSCP 48 IP precedence 7 = DSCP 56
DSCP to CoS map (CoS set from DSCP values)	DSCP 0–7 = CoS 0 DSCP 8–15 = CoS 1 DSCP 16–23 = CoS 2 DSCP 24–31 = CoS 3 DSCP 32–39 = CoS 4 DSCP 40–47 = CoS 5 DSCP 48–55 = CoS 6 DSCP 56–63 = CoS 7
Marked-down DSCP from DSCP map	Marked-down DSCP value equals original DSCP value (no markdown)
Policers	None
Policy maps	None

Table 32-2 PFC QoS Default Configuration (continued)

Feature	Default Value
With PFC QoS enabled	
Ingress LAN port trust state	Untrusted
2q2t transmit-queue size ratio	Low priority: 80%; high priority: 20%
1p1q0t receive-queue size ratio	Standard: 80%; strict priority: 20%
1p2q2t transmit-queue size ratio	Low priority: 70%; high priority: 15%; strict priority: 15%
1p2q1t transmit-queue size ratio	Low priority: 70%; high priority: 15%; strict priority: 15%
1p2q1t standard transmit-queue low:high priority bandwidth allocation ratio	100:255
2q2t, **1p2q2t**, and **1p2q1t** standard transmit-queue low:high priority bandwidth allocation ratio	5:255
1p3q1t standard transmit-queue low:medium:high-priority bandwidth allocation ratio	100:150:255
1q4t/2q2t receive and transmit queue CoS value/drop-threshold mapping	• Receive queue 1/drop threshold 1(50%) and transmit queue 1/drop threshold 1 (80%): CoS 0 and 1 • Receive queue 1/drop threshold 2 (60%) and transmit queue 1/drop threshold 2 (100%): CoS 2 and 3 • Receive queue 1/drop threshold 3 (80%) and transmit queue 2/drop threshold 1 (80%): CoS 4 and 5 • Receive queue 1/drop threshold 4 (100%) and transmit queue 2/drop threshold 2 (100%): CoS 6 and 7
1q2t port receive-queue CoS value/drop-threshold mapping and threshold percentages	• Receive queue 1/drop threshold 1: – CoS 0, 1, 2, 3, and 4 – Drop threshold: 80% • Receive queue 1/drop threshold 2: – CoS 5, 6, and 7 – Drop threshold: 100% (not configurable) **Note** Transmit queues same as **1p1q4t/1p2q2t**

Table 32-2 PFC QoS Default Configuration (continued)

Feature	Default Value
1p1q4t/1p2q2t port receive and transmit queue CoS value/drop-threshold mapping and threshold percentages:	• Strict-priority receive queue and strict-priority transmit queue: CoS 5 • Receive queue 1/drop threshold 1 and transmit queue 1/drop threshold 1: – CoS 0 and 1 – Transmit queue low and high WRED-drop thresholds: 40% and 70% • Receive queue 1/drop threshold 2 and transmit queue 1/drop threshold 2: – CoS 2 and 3 – Transmit queue low and high WRED-drop thresholds: 70% and 100% • Receive queue 1/drop threshold 3 and transmit queue 2/drop threshold 1: – CoS 4 and 6 – Transmit queue low and high WRED-drop thresholds: 40% and 70% • Receive queue 1/drop threshold 4 and transmit queue 2/drop threshold 2: – CoS 7 – Transmit queue low and high WRED-drop thresholds: 70% and 100%
1p1q0t receive queue CoS value mapping	• Receive queue 1 (standard) nonconfigurable 100% tail-drop threshold: CoS 0, 1, 2, 3, 4, 6, and 7 • Receive queue 2 (strict priority): CoS 5
1p3q1t transmit queue CoS value/drop-threshold mapping	• Transmit queue 1 (standard low priority) tail-drop threshold: – CoS 0 and 1 – Low and high WRED-drop threshold: 70% and 100% • Transmit queue 2 (standard medium priority) tail-drop threshold: – CoS 2, 3, and 4 – Low and high WRED-drop threshold: 70% and 100% • Transmit queue 3 (standard high priority) tail-drop threshold: – CoS 6 and 7 – Low and high WRED-drop threshold: 70% and 100% • Transmit queue 4 (strict priority): CoS 5

Table 32-2 PFC QoS Default Configuration (continued)

Feature	Default Value
1p1q8t receive queue port CoS value/drop-threshold mapping	• Receive queue 1 (standard) WRED-drop threshold: CoS 0, 1, 2, 3, 4, 6, and 7: – Drop threshold 1: CoS 0 Low WRED threshold: 40% High WRED-drop threshold: 70% – Drop threshold 2: CoS 1 Low WRED threshold: 40% High WRED-drop threshold: 70% – Drop threshold 3: CoS 2 Low WRED threshold: 50% High WRED-drop threshold: 80% – Drop threshold 4: CoS 3 Low WRED threshold: 50% High WRED-drop threshold: 80% – Drop threshold 5: CoS 4 Low WRED threshold: 60% High WRED-drop threshold: 90% – Drop threshold 6: CoS 6 Low WRED threshold: 60% High WRED-drop threshold: 90% – Drop threshold 6: CoS 7 Low WRED threshold: 70% High WRED-drop threshold: 100% • Receive queue 2 (strict priority): CoS 5
1p2q1t transmit queue port CoS value/drop-threshold mapping	• Transmit queue 1 (standard low priority) WRED-drop threshold: – CoS 0, 1, 2, and 3 – Low WRED threshold: 70% – High WRED-drop threshold: 100% • Transmit queue 2 (standard high priority) WRED-drop threshold: – CoS 4, 6, or 7 – Low WRED threshold: 70% – High WRED-drop threshold: 100% • Transmit queue 3 (strict-priority): CoS 5
PFC QoS Data Export	
Global PFC QoS data export	Disabled
Per port PFC QoS data export	Disabled
Per named aggregate policer PFC QoS data export	Disabled
Per class map policer PFC QoS data export	Disabled
PFC QoS data export time interval	300 seconds

Table 32-2 PFC QoS Default Configuration (continued)

Feature	Default Value
Export destination	Not configured
PFC QoS data export field delimiter	Pipe character (|)
With PFC QoS disabled	
Ingress LAN port trust state	**trust-dscp**
Receive-queue drop-threshold percentages	All thresholds set to 100%
Transmit-queue drop-threshold percentages	All thresholds set to 100%
Transmit-queue bandwidth allocation ratio	255:1
Transmit-queue size ratio	Low priority: 100% (other queues not used)
CoS value/drop threshold mapping	All CoS values mapped to the low-priority queue

PFC QoS Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring PFC QoS:

- With an MSFC2, Release 12.1(13)E and later releases support the **match protocol** class map command, which configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in software on the MSFC2. To configure NBAR, refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

  Earlier releases provide PFC QoS and Layer 3 switching in hardware, which prevents support of the **match protocol** class map command except for traffic being processed in software on the MSFC.
- PFC QoS does not support the **match cos, match any, match classmap, match destination-address, match input-interface, match mpls, match qos-group**, or **match source-address** class map commands.
- PFC QoS supports class maps that contain a ***single*** **match** command.
- PFC QoS filters only by access lists, dscp values, or IP precedence values.
- PFC QoS does not support the **class** *class_name* **destination-address, class** *class_name* **input-interface, class** *class_name* **protocol, class** *class_name* **qos-group**, or **class** *class_name* **source-address** policy map commands.
- PFC QoS does not support the **bandwidth, priority, queue-limit,** or **random-detect** policy map class commands.
- With Release 12.1(12c)E1 and later releases, PFC QoS supports the **set ip dscp** and **set ip precedence** policy map class commands (see the "Configuring Policy Map Class Actions" section on page 32-42). With Release 12.1(12c)E1 and later releases, PFC QoS does not support the **set mpls experimental** or **set qos-group** policy map class commands. With earlier releases, PFC QoS does not support any **set** policy map class commands.
- With Release 12.1(11b)E1 and later releases, OSM QoS supports the **set mpls experimental** policy map class command. Refer to the following publication for information about OSM QoS:

  http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/cfgnotes/osm_inst/index.htm
- PFC QoS does not support the **output** service-policy keyword.
- PFC QoS has the following hardware granularity for CIR and PIR rate values:

CIR and PIR Rate Value Range	Granularity
32768 to 2097152 (2 Mbps)	32768 (32 Kb)
2097153 to 4194304 (4 Mbps)	65536 (64 Kb)
4194305 to 8388608 (8 Mbps)	131072 (128 Kb)
8388609 to 16777216 (16 Mbps)	262144 (256 Kb)
16777217 to 33554432 (32 Mbps)	524288 (512 Kb)
33554433 to 67108864 (64 Mbps)	1048576 (1 Mb)
67108865 to 134217728 (128 Mbps)	2097152 (2 Mb)
134217729 to 268435456 (256 Mbps)	4194304 (4 Mb)
268435457 to 536870912 (512 Mbps)	8388608 (8 Mb)
536870913 to 1073741824 (1 Gps)	16777216 (16 Mb)
1073741825 to 2147483648 (2 Gps)	33554432 (32 Mb)
2147483649 to 4294967296 (4 Gps)	67108864 (64 Mb)

Within each range, PFC QoS programs the PFC hardware with rate values that are multiples of the granularity values.

- PFC QoS has the following hardware granularity for CIR and PIR token bucket (burst) sizes:

CIR and PIR Token Bucket Size Range	Granularity
1 to 32768 (32 KB)	1024 (1 KB)
32769 to 65536 (64 KB)	2048 (2 KB)
65537 to 131072 (128 KB)	4096 (4 KB)
131073 to 262144 (256 KB)	8196 (8 KB)
262145 to 524288 (512 KB)	16392 (16 KB)
524289 to 1048576 (1 MB)	32768 (32 KB)
1048577 to 2097152 (2 MB)	65536 (64 KB)
2097153 to 4194304 (4 MB)	131072 (128 KB)
4194305 to 8388608 (8 MB)	262144 (256 KB)
8388609 to 16777216 (16 MB)	524288 (512 KB)
16777217 to 33554432 (32 MB)	1048576 (1 MB)

Within each range, PFC QoS programs the PFC hardware with token bucket sizes that are multiples of the granularity values.

- For these commands, PFC QoS applies identical configuration to all LAN ports controlled by the same application-specific integrated circuit (ASIC):
  - rcv-queue queue-limit
  - wrr-queue queue-limit
  - wrr-queue bandwidth (except Gigabit Ethernet LAN ports)
  - priority-queue cos-map

- rcv-queue cos-map
- wrr-queue cos-map
- wrr-queue threshold
- rcv-queue threshold
- wrr-queue random-detect
- wrr-queue random-detect min-threshold
- wrr-queue random-detect max-threshold

Configuring PFC QoS

These sections describe how to configure PFC QoS on the Catalyst 6500 series switches:

- Enabling PFC QoS Globally, page 32-31
- Enabling Queueing-Only Mode, page 32-32
- Creating Named Aggregate Policers, page 32-33
- Configuring a PFC QoS Policy, page 32-35
- Enabling or Disabling Microflow Policing, page 32-48
- Enabling Microflow Policing of Bridged Traffic, page 32-48
- Enabling or Disabling PFC Features on an Interface, page 32-49
- Enabling VLAN-Based PFC QoS on Layer 2 LAN Ports, page 32-50
- Configuring the Trust State of Ethernet LAN and OSM Ingress Ports, page 32-51
- Configuring the Ingress LAN Port CoS Value, page 32-52
- Configuring LAN-Port Drop Threshold Percentages, page 32-52
- Enabling and Disabling WRED-Drop Thresholds, page 32-57
- Mapping CoS Values to LAN-Port Drop Thresholds, page 32-57
- Allocating Bandwidth Between LAN-Port Transmit Queues, page 32-62
- Setting the Receive-Queue Size Ratio on a 1p1q0t or 1p1q8t Ingress LAN Ports, page 32-62
- Setting the LAN-Port Transmit-Queue Size Ratio, page 32-63
- Configuring DSCP Value Maps, page 32-64
- Configuring PFC QoS Statistics Data Export, page 32-68

Note
- PFC QoS processes both unicast and multicast traffic.
- With Release 12.1(11b)E and later releases, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

Enabling PFC QoS Globally

To enable PFC QoS globally, perform this task:

	Command	Purpose
Step 1	`Router(config)# mls qos`	Enables PFC QoS globally on the switch.
	`Router(config)# no mls qos`	Disables PFC QoS globally on the switch.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos`	Verifies the configuration.

This example shows how to enable PFC QoS globally:

```
Router# configure terminal
Router(config)# mls qos
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos
  QoS is enabled globally
  Microflow QoS is enabled globally

QoS global counters:
    Total packets: 544393
    IP shortcut packets: 1410
    Packets dropped by policing: 0
    IP packets with TOS changed by policing: 467
    IP packets with COS changed by policing: 59998
    Non-IP packets with COS changed by policing: 0
```

Enabling Queueing-Only Mode

To enable queueing-only mode on the switch, perform this task:

	Command	Purpose
Step 1	`Router(config)# mls qos queueing-only`	Enables queueing-only mode on the switch.
	`Router(config)# no mls qos queueing-only`	Disables PFC QoS globally on the switch. **Note** You cannot disable queueing-only mode separately.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos`	Verifies the configuration.

When you enable queueing-only mode, the switch does the following:

- Disables marking and policing globally
- Configures all ports to trust Layer 2 CoS

Note The switch applies the port CoS value to untagged ingress traffic and to traffic that is received through ports that cannot be configured to trust CoS.

This example shows how to enable queueing-only mode:

```
Router# configure terminal
Router(config)# mls qos queueing-only
Router(config)# end
Router#
```

Creating Named Aggregate Policers

To create a named aggregate policer (see the "Policers" section on page 32-19), perform this task:

Command	Purpose
Router(config)# **mls qos aggregate-policer** *policer_name bits_per_second normal_burst_bytes* [*maximum_burst_bytes*] [**pir**[1] *peak_rate_bps*] [[[**conform-action** {**drop** | **set-dscp-transmit**[2] *dscp_value* | **set-prec-transmit**[2] *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action**[1] {**drop** | **policed-dscp** | **transmit**}]	Creates a named aggregate policer.
Router(config)# **no mls qos aggregate-policer** *policer_name*	Deletes a named aggregate policer.

[1] Supported only with PFC2.

[2] With PFC2, the **set-dscp-transmit** and **set-prec-transmit** keywords are only supported for IP traffic.

Note With PFC2, aggregate policers can be applied to ingress interfaces on multiple modules, but aggregate policing works independently on each DFC-equipped switching module and independently on the PFC2, which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate policing statistics for each DFC-equipped switching module and for the PFC2 and any non-DFC-equipped switching modules supported by the PFC2.

When creating a named aggregate policer, note the following:

- Policing uses the Layer 3 packet size.
- See the "PFC QoS Configuration Guidelines and Restrictions" section on page 32-29 for information about rate and burst size granularity.
- The valid range of values for the CIR *bits_per_second* parameter is as follows:
  - Minimum—32 kilobits per second, entered as 32000
  - Maximum—4 gigabits per second, entered as 4000000000
- The *normal_burst_bytes* parameter sets the CIR token bucket size.
- The *maximum_burst_bytes* parameter sets the PIR token bucket size.
- When configuring the size of a token bucket, note the following:
  - The minimum token bucket size is 1 kilobyte, entered as 1000 (the *maximum_burst_bytes* parameter must be set larger than the *normal_burst_bytes* parameter)
  - The maximum token bucket size is approximately 32 megabytes, entered as 31250000
  - To sustain a specific rate, set the token bucket size to be at least the rate value divided by 4000, because tokens are removed from the bucket every 1/4000th of a second (0.25 ms).

  - Because the token bucket must be large enough to hold at least one frame, set the parameter larger than the maximum Layer 3 packet size of the traffic being policed.
  - For TCP traffic, configure the token bucket size as a multiple of the TCP window size, with a minimum value at least twice as large as the maximum Layer 3 packet size of the traffic being policed.

  The *maximum_burst_bytes* parameter is supported with PFC2. The *maximum_burst_bytes* parameter is not supported with PFC, but can be entered with a value equal to the *normal_burst_bytes* parameter.

- The valid range of values for the **pir** *bits_per_second* parameter is as follows:
  - Minimum—32 kilobits per second, entered as 32000 (the value cannot be smaller than the CIR *bits_per_second* parameters)
  - Maximum—4 gigabits per second, entered as 4000000000

  The **pir** *bits_per_second* parameter is supported with the PFC2. The **pir** *bits_per_second* parameter is not supported with the PFC1 but can be entered with the PFC1 if the value is equal to the CIR *bits_per_second* parameter.

- (Optional) You can specify a conform action for matched in-profile traffic as follows:
  - The default conform action is **transmit**, which sets the policy map class trust state to *trust DSCP* unless the policy map class contains a **trust** command (see the "Policy Maps" section on page 32-18 and the "Configuring Policy Map Class Actions" section on page 32-42).
  - To set PFC QoS labels in untrusted traffic, enter the **set-dscp-transmit** keyword to mark matched untrusted traffic with a new DSCP value or enter the **set-prec-transmit** keyword to mark matched untrusted traffic with a new IP precedence value (with the PFC2, the **set-dscp-transmit** and **set-prec-transmit** keywords are only supported for IP traffic). PFC QoS sets egress ToS and CoS from the configured value.
  - Enter the **drop** keyword to drop all matched traffic.

  Note When you configure **drop** as the conform action, PFC QoS configures **drop** as the exceed action and the violate action.

- (Optional) For traffic that exceeds the CIR, you can specify an exceed action as follows:
  - The default exceed action is **drop**, except with a *maximum_burst_bytes* parameter (**drop** is not supported with a *maximum_burst_bytes* parameter).

  Note When the exceed action is **drop**, PFC QoS ignores any configured violate action.

  - Enter the **policed-dscp-transmit** keyword to cause all matched out-of-profile traffic to be marked down as specified in the markdown map (see the "Configuring DSCP Markdown Values" section on page 32-66).

  Note When you create a policer that does not use the **pir** keyword and the *maximum_burst_bytes* parameter is equal to the *normal_burst_bytes* parameter (which is the case if you do not enter the *maximum_burst_bytes* parameter), the **exceed-action policed-dscp-transmit** keywords cause PFC QoS to mark traffic down as defined by the **policed-dscp max-burst** markdown map.

- (Optional) For traffic that exceeds the PIR, you can specify a violate action as follows:
  - To mark traffic without policing, enter the **transmit** keyword to transmit all matched out-of-profile traffic.
  - The default violate action is equal to the exceed action.
  - Enter the **policed-dscp-transmit** keyword to cause all matched out-of-profile traffic to be marked down as specified in the markdown map (see the "Configuring DSCP Markdown Values" section on page 32-66).
  - For marking without policing, enter the **transmit** keyword to transmit all matched out-of-profile traffic.

  The **violate-action** keyword is not supported with the PFC1, but the keyword can be entered with a PFC1 if the parameters match the **exceed-action** parameters.

This example shows how to create a named aggregate policer with a 1-Mbps rate limit and a 10-MB burst size that transmits conforming traffic and marks down out-of-profile traffic:

```
Router(config)# mls qos aggregate-policer aggr-1 1000000 10000000 conform-action transmit
exceed-action policed-dscp-transmit
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos aggregate-policer aggr-1
ag1 1000000 1000000 conform-action transmit exceed-action policed-dscp-transmit AgId=0
[pol4]
Router#
```

The output displays the following:

- The **AgId** parameter displays the hardware policer ID.
- The policy maps that use the policer are listed in the square brackets ([]).

Configuring a PFC QoS Policy

These sections describe PFC QoS policy configuration:

- PFC QoS Policy Configuration Overview, page 32-36
- Configuring MAC-Layer Named Access Lists (Optional), page 32-37
- Configuring a Class Map (Optional), page 32-38
- Verifying Class Map Configuration, page 32-39
- Configuring a Policy Map, page 32-40
- Verifying Policy Map Configuration, page 32-46
- Attaching a Policy Map to an Interface, page 32-47

Note PFC QoS policies process both unicast and multicast traffic.

PFC QoS Policy Configuration Overview

Note To mark traffic without limiting bandwidth utilization, create a policer that uses the **transmit** keywords for both conforming and nonconforming traffic.

These commands configure traffic classes and the policies to be applied to those traffic classes and attach the policies to ports:

- **access-list** (Optional for IP traffic. You can filter IP traffic with **class-map** commands.):
  - PFC QoS supports these access list types:

Protocol	Numbered Access Lists?	Extended Access Lists?	Named Access Lists?
IP	Yes: 1 to 99 1300 to 1999	Yes: 100 to 199 2000 to 2699	Yes
IPX[1]	Yes: 800 to 899	Yes: 900 to 999	Yes
MAC Layer[1]	No	No	Yes[2]

[1] Supported with Release 12.1(1)E and later.

[2] Supported with Release 12.1(1)E and later; see the "Configuring MAC-Layer Named Access Lists (Optional)" section on page 32-37.

  - In Release 12.1(19)E and later releases, PFC QoS supports time-based Cisco IOS ACLs.
  - In Release 12.1(1)E and later releases, PFC QoS supports IPX access lists that contain a *source-network* parameter and the optional *destination-network* and *destination-node* parameters. PFC QoS does not support IPX access control lists that contain other parameters (for example, *source-node*, *protocol*, *source-socket*, *destination-socket*, or *service-type*).
  - Except for MAC-Layer named access lists (see the "Configuring MAC-Layer Named Access Lists (Optional)" section on page 32-37), refer to the *Cisco IOS Security Configuration Guide*, Release 12.1, "Traffic Filtering and Firewalls," "Access Control Lists: Overview and Guidelines," at this URL:

    http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/index.htm
  - See Chapter 23, "Configuring Network Security," for additional information about ACLs on the Catalyst 6500 series switches.
- **class-map** (optional)—Enter the **class-map** command to define one or more traffic classes by specifying the criteria by which traffic is classified (see the "Configuring a Class Map (Optional)" section on page 32-38).

  Note You can also create class-maps during policy map creation with the **policy-map class** command (see the "Creating a Policy Map Class and Configuring Filtering" section on page 32-41).
- **policy-map**—Enter the **policy-map** command to define the following:
  - New class maps
  - Policy map class trust mode

- Aggregate policing and marking
- Microflow policing and marking

- **service-policy**—Enter the **service-policy** command to attach a policy map to an interface.

Configuring MAC-Layer Named Access Lists (Optional)

In Release 12.1(1)E and later releases, you can configure named access lists that filter DECnet, AppleTalk, VINES, or XNS traffic based on Layer 2 addresses.

To configure a MAC-Layer named access list, perform this task:

	Command	Purpose
Step 1	`Router(config)# mac access-list extended list_name`	Configures a MAC-Layer named access list.
	`Router(config)# no mac access-list extended list_name`	Deletes a MAC-Layer named access list.
Step 2	`Router(config-ext-macl)# {permit | deny} {src-mac-mask | any} {dest-mac-mask | any} [aarp | amber | appletalk | diagnostic | decnet-iv | dec-spanning | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-ip | vines-echo | xns]`	Configures an access control entry (ACE) in a MAC-Layer named access list.
	`Router(config-ext-macl)# no {permit | deny} {src-mac-mask | any} {dest-mac-mask | any} [aarp | amber | appletalk | diagnostic | decnet-iv | dec-spanning | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-ip | vines-echo | xns]`	Deletes an ACE from a MAC-Layer named access list.

When configuring an entry in a MAC-Layer access list, note the following:

- You can enter MAC addresses as three 4-byte values in dotted hexadecimal format. For example, 0030.9629.9f84.
- You can enter MAC address masks as three 4-byte values in dotted hexadecimal format. Use 1 bits as wildcards. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- Entries without a protocol parameter match any protocol.
- Access lists entries are scanned in the order you enter them. The first matching entry is used. To improve performance, place the most commonly used entries near the beginning of the access list.
- An implicit **deny any any** entry exists at the end of an access list unless you include an explicit **permit any any** entry at the end of the list.
- All new entries to an existing list are placed at the end of the list. You cannot add entries to the middle of a list.

This list shows the ethertype values matched by the protocol keywords:

- 0x0600—xns-idp—Xerox XNS IDP
- 0x0BAD—vines-ip—Banyan VINES IP
- 0x0baf—vines-echo—Banyan VINES Echo
- 0x6000—etype-6000—DEC unassigned, experimental

- 0x6001—mop-dump—DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
- 0x6002—mop-console—DEC MOP Remote Console
- 0x6003—decnet-iv—DEC DECnet Phase IV Route
- 0x6004—lat—DEC Local Area Transport (LAT)
- 0x6005—diagnostic—DEC DECnet Diagnostics
- 0x6007—lavc-sca—DEC Local-Area VAX Cluster (LAVC), SCA
- 0x6008—amber—DEC AMBER
- 0x6009—mumps—DEC MUMPS
- 0x8038—dec-spanning—DEC LANBridge Management
- 0x8039—dsm—DEC DSM/DDP
- 0x8040—netbios—DEC PATHWORKS DECnet NETBIOS Emulation
- 0x8041—msdos—DEC Local Area System Transport
- 0x8042—etype-8042—DEC unassigned
- 0x809B—appletalk—Kinetics EtherTalk (AppleTalk over Ethernet)
- 0x80F3—aarp—Kinetics AppleTalk Address Resolution Protocol (AARP)

This example shows how to create a MAC-Layer access list named **mac_layer** that denies **dec-phase-iv** traffic with source address 0000.4700.0001 and destination address 0000.4700.0009, but permits all other traffic:

```
Router(config)# mac access-list extended mac_layer
Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv
Router(config-ext-macl)# permit any any
```

Configuring a Class Map (Optional)

These sections describe class map configuration:

- Creating a Class Map, page 32-38
- Configuring Filtering in a Class Map, page 32-39

Note You can also create class maps during policy map creation with the **policy-map class** command (see the "Creating a Policy Map Class and Configuring Filtering" section on page 32-41).

Creating a Class Map

To create a class map, perform this task:

Command	Purpose
`Router(config)# class-map class_name`	Creates a class map.
`Router(config)# no class-map class_name`	Deletes a class map.

Configuring Filtering in a Class Map

Note Except for MAC-Layer ACLs (see the "Configuring MAC-Layer Named Access Lists (Optional)" section on page 32-37), access lists are not documented in this publication. See the reference under **access-list** in the "Configuring a PFC QoS Policy" section on page 32-35.

To configure filtering in a class map, perform one of these tasks:

Command	Purpose
Router(config-cmap)# **match access-group name** *acl_index_or_name*	(Optional) Configures the class map to filter using an ACL.
Router(config-cmap)# **no match access-group name** *acl_index_or_name*	Clears the ACL configuration from the class map.
Router (config-cmap)# **match ip precedence** *ipp_value1* [*ipp_value2* [*ipp_valueN*]]	(Optional—for IP traffic only) Configures the class map to filter on up to eight IP precedence values.
Router (config-cmap)# **no match ip precedence** *ipp_value1* [*ipp_value2* [*ipp_valueN*]]	Clears configured IP precedence values from the class map.
Router (config-cmap)# **match ip dscp** *dscp_value1* [*dscp_value2* [*dscp_valueN*]]	(Optional—for IP traffic only) Configures the class map to filter on up to eight DSCP values.
Router (config-cmap)# **no match ip dscp** *dscp_value1* [*dscp_value2* [*dscp_valueN*]]	Clears configured DSCP values from the class map.

Note

- With an MSFC2, Release 12.1(13)E and later releases support the **match protocol** class map command, which configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in software on the MSFC2. To configure NBAR, refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

  Earlier releases provide PFC QoS and Layer 3 switching in hardware, which prevents support of the **match protocol** class map command except for traffic being processed in software on the MSFC.
- PFC QoS supports class maps that contain a single **match** command.
- PFC QoS does not support the **match cos, match any, match classmap, match destination-address, match input-interface, match mpls, match qos-group**, and **match source-address** class map commands.
- Catalyst 6500 series switches do not detect the use of unsupported commands until you attach a policy map to an interface (see the "Attaching a Policy Map to an Interface" section on page 32-47).

Verifying Class Map Configuration

To verify class map configuration, perform this task:

	Command	Purpose
Step 1	Router (config-cmap)# **end**	Exits configuration mode.
Step 2	Router# **show class-map** *class_name*	Verifies the configuration.

This example shows how to create a class map named **ipp5** and how to configure filtering to match traffic with IP precedence 5:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show class-map ipp5
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5

Router#
```

Configuring a Policy Map

You can attach only one policy map to an interface. Policy maps can contain one or more policy map classes, each with different policy map commands.

Configure a separate policy map class in the policy map for each type of traffic that an interface receives. Put all commands for each type of traffic in the same policy map class. PFC QoS does not attempt to apply commands from more than one policy map class to matched traffic.

These sections describe policy map configuration:

- Creating a Policy Map, page 32-40
- Creating a Policy Map Class and Configuring Filtering, page 32-41
- Configuring Policy Map Class Actions, page 32-42

Creating a Policy Map

To create a policy map, perform this task:

Command	Purpose
`Router(config)# policy-map policy_name`	Creates a policy map.
`Router(config)# no policy-map policy_name`	Deletes the policy map.

Creating a Policy Map Class and Configuring Filtering

Note

- With an MSFC2, Release 12.1(13)E and later releases support the **class** *class_name* **protocol** policy map command, which configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in software on the MSFC2. To configure NBAR, refer to this publication:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm

  Earlier releases provide PFC QoS and Layer 3 switching in hardware, which prevents support of the **class** *class_name* **protocol** policy map command except for traffic being processed in software on the MSFC.
- PFC QoS does not support the **class** *class_name* **destination-address**, **class** *class_name* **input-interface**, **class** *class_name* **qos-group**, and **class** *class_name* **source-address** policy map commands.
- PFC QoS does not detect the use of unsupported commands until you attach a policy map to an interface (see the "Attaching a Policy Map to an Interface" section on page 32-47).

Policy maps can contain one or more policy map classes. Enter one of these **class** commands to create a policy map class and configure filtering in it.

To create a policy map class and configure it to filter with an already defined class map, perform this task:

Command	Purpose
Router(config-pmap)# **class** *class_name*	Creates a policy map class and configures it to filter with a class map (see the "Creating a Class Map" section on page 32-38). **Note** PFC QoS supports class maps that contain a single **match** command.
Router(config-pmap)# **no class** *class_name*	Clears use of the class map.

To create a policy map class and a class map simultaneously, perform this task:

Command	Purpose
Router(config-pmap)# **class** *class_name* {**access-group** *acl_index_or_name* | **dscp** *dscp_1* [*dscp_2* [*dscp_N*]] | **precedence** *ipp_1* [*ipp_2* [*ipp_N*]]}	Creates a policy map class and creates a class map and configures the policy map class to filter with the class map. **Note** This command creates a class map that can be used in other policy maps.
Router(config-pmap)# **no class** *class_name*	Clears use of the class map (does not delete the class map).

Note

- Put all trust-state and policing commands for each type of traffic in the same policy map class.
- PFC QoS does not attempt to apply commands from more than one policy map class to traffic.

Configuring Policy Map Class Actions

When configuring policy map class actions, note the following:

- For hardware-switched traffic, PFC QoS does not support the **bandwidth, priority, queue-limit**, or **random-detect** policy map class commands. You can configure these commands because they can be used for software-switched traffic.
- With Release 12.1(12c)E1 and later releases, PFC QoS does not support the **set mpls** or **set qos-group** policy map class commands. With earlier releases, PFC QoS does not support any **set** policy map class commands.
- With Release 12.1(12c)E1 and later releases, PFC QoS supports the **set ip dscp** and **set ip precedence** policy map class commands (see the "Configuring Policy Map Class Marking" section on page 32-42).
- With Release 12.1(12c)E1 and later releases, you cannot do all three of the following in a policy map class:
  - Mark traffic with the **set ip dscp** or **set ip precedence** commands
  - Configure the trust state
  - Configure policing

  In a policy map class, you can either mark untrusted traffic with the **set ip dscp** or **set ip precedence** commands or do one or both of the following:
  - Configure the trust state
  - Configure policing

Note When configure policing, you can mark traffic with policing keywords (see the "Configuring Policy Map Class Policing" section on page 32-43).

These sections describe policy map class action configuration:

- Configuring Policy Map Class Marking, page 32-42
- Configuring the Policy Map Class Trust State, page 32-43
- Configuring Policy Map Class Policing, page 32-43

Configuring Policy Map Class Marking

With Release 12.1(12c)E1 and later releases, PFC QoS supports policy map class marking for untrusted traffic with the **set ip dscp** and **set ip precedence** policy map class commands.

To configure policy map class marking for untrusted traffic, perform this task:

Command	Purpose
Router(config-pmap-c)# **set ip** {**dscp** *dscp_value* | **precedence** *ip_precedence_value*}	Configures the policy map class to mark matched untrusted traffic with the configured DSCP or IP precedence value.
Router(config-pmap-c)# **no set ip** {**dscp** *dscp_value* | **precedence** *ip_precedence_value*}	Clears the marking configuration.

Configuring the Policy Map Class Trust State

To configure the policy map class trust state, perform this task:

Command	Purpose
`Router(config-pmap-c)# trust {cos | dscp | ip-precedence}`	Configures the policy map class trust state, which selects the value that PFC QoS uses as the source of the internal DSCP value (see the "Internal DSCP Values" section on page 32-17).
`Router(config-pmap-c)# no trust`	Reverts to the default policy-map class trust state (untrusted).

When configuring the policy map class trust state, note the following:

- Enter the **no trust** command to use the trust state configured on the ingress port (this is the default).
- With the **cos** keyword, PFC QoS sets the internal DSCP value from received or ingress port CoS (see the "Mapping Received CoS Values to Internal DSCP Values" section on page 32-64).
- With the **dscp** keyword, PFC QoS uses received DSCP.
- With the **ip-precedence** keyword, PFC QoS sets DSCP from received IP precedence (see the "Mapping Received IP Precedence Values to Internal DSCP Values" section on page 32-65).

Configuring Policy Map Class Policing

When you configure policy map class policing, note the following:

- PFC QoS does not support the **set-qos-transmit** policer keyword.
- PFC QoS does not support the **set-dscp-transmit** or **set-prec-transmit** keywords as arguments to the **exceed-action** keyword.
- PFC QoS does not detect the use of unsupported keywords until you attach a policy map to an interface (see the "Attaching a Policy Map to an Interface" section on page 32-47).

These sections describe configuration of policy map class policing:

- Using a Named Aggregate Policer, page 32-43
- Configuring a Per-Interface Policer, page 32-44

Note Policing with the **conform-action transmit** keywords sets the port trust state of matched traffic to trust DSCP or to the trust state configured by a **trust** command in the policy map class.

Using a Named Aggregate Policer

To use a named aggregate policer (see the "Creating Named Aggregate Policers" section on page 32-33), perform this task:

Command	Purpose
`Router(config-pmap-c)# police aggregate` *`aggregate_name`*	Configures the policy map class to use a previously defined named aggregate policer.
`Router(config-pmap-c)# no police aggregate` *`aggregate_name`*	Clears use of the named aggregate policer.

Configuring a Per-Interface Policer

To configure a per-interface policer (see the "Policers" section on page 32-19), perform this task:

Command	Purpose
Router(config-pmap-c)# **police** [**flow**] *bits_per_second normal_burst_bytes* [*maximum_burst_bytes*] [**pir**[1] *peak_rate_bps*] [[[**conform-action** {**drop** | **set-dscp-transmit**[2] *dscp_value* | **set-prec-transmit**[2] *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action**[1] {**drop** | **policed-dscp** | **transmit**}]	Creates a per-interface policer and configures the policy map class to use it.
Router(config-pmap-c)# **no police** [**flow**] *bits_per_second normal_burst_bytes* [*maximum_burst_bytes*] [**pir** *peak_rate_bps*] [[[**conform-action** {**drop** | **set-dscp-transmit** *dscp_value* | **set-prec-transmit** *ip_precedence_value* | **transmit**}] **exceed-action** {**drop** | **policed-dscp** | **transmit**}] **violate-action** {**drop** | **policed-dscp** | **transmit**}]	Deletes the per-interface policer from the policy map class.

[1] Supported only with PFC2. Not supported in microflow policers (the **flow** keyword configures a microflow policer).

[2] With PFC2, the **set-dscp-transmit** and **set-prec-transmit** keywords are only supported for IP traffic.

When configuring a per-interface policer, note the following:

- Policing uses the Layer 3 packet size.
- See the "PFC QoS Configuration Guidelines and Restrictions" section on page 32-29 for information about rate and burst size granularity.
- You can enter the **flow** keyword to define a microflow policer. During microflow policing, the following occurs:
  - PFC QoS considers IPX traffic with same source network, destination network, and destination node to be part of the same flow, including traffic with different source nodes or sockets.
  - PFC QoS considers MAC-Layer traffic with the same protocol and the same source and destination MAC-Layer addresses to be part of the same flow, including traffic with different ethertypes.
  - Microflow policers do not support the *maximum_burst_bytes* parameter, the **pir** *bits_per_second* keyword and parameter, or the **violate-action** keyword.
- The valid range of values for the CIR *bits_per_second* parameter is as follows:
  - Minimum—32 kilobits per second, entered as 32000
  - Maximum—4 gigabits per second, entered as 4000000000
- The *normal_burst_bytes* parameter sets the CIR token bucket size.
- The *maximum_burst_bytes* parameter sets the PIR token bucket size (not supported with the **flow** keyword)
- When configuring the size of a token bucket, note the following:
  - The minimum token bucket size is 1 kilobyte, entered as 1000 (the *maximum_burst_bytes* parameter must be set larger than the *normal_burst_bytes* parameter)
  - The maximum token bucket size is approximately 32 megabytes, entered as 31250000
  - To sustain a specific rate, set the token bucket size to be at least the rate value divided by 4000, because tokens are removed from the bucket every 1/4000th of a second (0.25 ms).

- Because the token bucket must be large enough to hold at least one frame, set the parameter larger than the maximum Layer 3 packet size of the traffic being policed.
- For TCP traffic, configure the token bucket size as a multiple of the TCP window size, with a minimum value at least twice as large as the maximum Layer 3 packet size of the traffic being policed.

The *maximum_burst_bytes* parameter is supported with the PFC2. The *maximum_burst_bytes* parameter is not supported with the PFC1, but the keyword can be entered with a value equal to the *normal_burst_bytes* parameter.

- (Not supported with the **flow** keyword.) The valid range of values for the **pir** *bits_per_second* parameter is as follows:
  - Minimum—32 kilobits per second, entered as 32000 (the value cannot be smaller than the CIR *bits_per_second* parameters)
  - Maximum—4 gigabits per second, entered as 4000000000

  The **pir** *bits_per_second* parameter is supported with the PFC2. The **pir** *bits_per_second* parameter is not supported with the PFC1, but can be entered with the PFC1 if the value is equal to the CIR *bits_per_second* parameter.
- (Optional) You can specify a conform action for matched in-profile traffic as follows:
  - The default conform action is **transmit**, which sets the policy map class trust state to *trust DSCP* unless the policy map class contains a **trust** command (see the "Policy Maps" section on page 32-18 and the "Configuring Policy Map Class Actions" section on page 32-42).
  - To set PFC QoS labels in untrusted traffic, you can enter the **set-dscp-transmit** keyword to mark matched untrusted traffic with a new DSCP value or enter the **set-prec-transmit** keyword to mark matched untrusted traffic with a new IP precedence value (with the PFC2, the **set-dscp-transmit** and **set-prec-transmit** keywords are only supported for IP traffic). PFC QoS sets egress ToS and CoS from the configured value.
  - You can enter the **drop** keyword to drop all matched traffic.
  - Ensure that aggregate and microflow policers that are applied to the same traffic each specify the same conform-action behavior.
- (Optional) For traffic that exceeds the CIR, you can specify an exceed action as follows:
  - For marking without policing, you can enter the **transmit** keyword to transmit all matched out-of-profile traffic.
  - The default exceed action is **drop**, except with a *maximum_burst_bytes* parameter (**drop** is not supported with a *maximum_burst_bytes* parameter).

Note When the exceed action is **drop**, PFC QoS ignores any configured violate action.

  - You can enter the **policed-dscp-transmit** keyword to cause all matched out-of-profile traffic to be marked down as specified in the markdown map (see the "Configuring DSCP Markdown Values" section on page 32-66).

Note When you create a policer that does not use the **pir** keyword and the *maximum_burst_bytes* parameter is equal to the *normal_burst_bytes* parameter (which is the case if you do not enter the *maximum_burst_bytes* parameter), the **exceed-action policed-dscp-transmit** keywords cause PFC QoS to mark traffic down as defined by the **policed-dscp max-burst** markdown map.

- (Optional—Not supported with the **flow** keyword) For traffic that exceeds the PIR, you can specify a violate action as follows:
  - For marking without policing, you can enter the **transmit** keyword to transmit all matched out-of-profile traffic.
  - The default violate action is equal to the exceed action.
  - You can enter the **policed-dscp-transmit** keyword to cause all matched out-of-profile traffic to be marked down as specified in the markdown map (see the "Configuring DSCP Markdown Values" section on page 32-66).

The **violate-action** keyword is not supported with the PFC1, but the keyword can be entered with the PFC1 if the parameters match the **exceed-action** parameters.

Note Aggregate policing works independently on each DFC-equipped switching module and independently on the PFC2, which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate policing statistics for each DFC-equipped switching module and for the PFC2 and any non-DFC-equipped switching modules supported by the PFC2.

This example shows how to create a policy map named **max-pol-ipp5** that uses the class-map named **ipp5**, which is configured to trust received IP precedence values and is configured with a maximum-capacity aggregate policer and with a microflow policer:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
```

Verifying Policy Map Configuration

To verify policy map configuration, perform this task:

	Command	Purpose
Step 1	`Router(config-pmap-c)# end`	Exits policy map class configuration mode. **Note** Enter additional **class** commands to create additional classes in the policy map.
Step 2	`Router# show policy-map policy_name`	Verifies the configuration.

This example shows how to verify the configuration:

```
Router# show policy-map max-pol-ipp5
 Policy Map max-pol-ipp5
  class  ipp5

  class ipp5
    police flow 10000000 10000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit
    trust precedence
    police 2000000000 2000000 2000000 conform-action set-prec-transmit 6 exceed-action
policed-dscp-transmit

Router#
```

Attaching a Policy Map to an Interface

Note PFC QoS does not support the **output** service-policy keyword.

To attach a policy map to an interface, perform this task:

	Command	Purpose
Step 1	`Router(config)#` **`interface`** `{{`**`vlan`** *`vlan_ID`*`} | {`*`type`*[1] *`slot/port`*`} | {`**`port-channel`** *`number`*`}}`	Selects the interface to configure.

Step 2	`Router(config-if)#` **`service-policy input`** *`policy_map_name`*
	`Router(config-if)#` **`no service-policy input`** *`policy_map_name`*
		Attaches a policy map to the input direction of the interface.
		Removes the policy map from the interface.

Step 3	`Router(config-if)#` **`end`**	Exits configuration mode.
Step 4	`Router#` **`show policy-map interface`** `{{`**`vlan`** *`vlan_ID`*`} | {`*`type`*[1] *`slot/port`*`} | {`**`port-channel`** *`number`*`}}`	Verifies the configuration.

[1] *type* = **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **ge-wan**, **pos**, or **atm**

Note Aggregate policing works independently on each DFC-equipped switching module and independently on the PFC2, which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate policing statistics for each DFC-equipped switching module and for the PFC2 and any non-DFC-equipped switching modules supported by the PFC2.

This example shows how to attach the policy map named **pmap1** to Fast Ethernet port 5/36:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# service-policy input pmap1
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show policy-map interface fastethernet 5/36
 FastEthernet5/36
  service-policy input: pmap1
    class-map: cmap1 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class cmap1
    police 8000 8000 conform-action transmit exceed-action drop
    class-map: cmap2 (match-any)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 2
        0 packets, 0 bytes
        5 minute rate 0 bps
  class cmap2
    police 8000 10000 conform-action transmit exceed-action drop
Router#
```

Enabling or Disabling Microflow Policing

To enable or disable microflow policing (see the "Policers" section on page 32-19), perform this task:

	Command	Purpose
Step 1	`Router(config)# mls qos flow-policing`	Enables microflow policing.
	`Router(config)# no mls qos flow-policing`	Disables microflow policing.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos`	Verifies the configuration.

This example shows how to disable microflow policing:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no mls qos flow-policing
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos | include Microflow
  Microflow QoS is disabled globally
Router#
```

Enabling Microflow Policing of Bridged Traffic

Note To apply microflow policing to multicast traffic, you must enter the **mls qos bridged** command on the Layer 3 multicast ingress interfaces.

By default, microflow policers affect only routed traffic. To enable microflow policing of bridged traffic on specified VLANs, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** {{**vlan** *vlan_ID*} | {*type*[1] *slot/port*}}	Selects the interface to configure.
Step 2	Router(config-if)# **mls qos bridged**	Enables microflow policing of bridged traffic, including bridge groups, on the VLAN.
	Router(config-if)# **no mls qos bridged**	Disables microflow policing of bridged traffic.
Step 3	Router(config-if)# **end**	Exits configuration mode.
Step 4	Router# **show mls qos**	Verifies the configuration.

[1] *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable microflow policing of bridged traffic on VLANs 3 through 5:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface range vlan 3 - 5
Router(config-if)# mls qos bridged
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos | begin Bridged QoS
Bridged QoS is enabled on the following interfaces:
    Vl3 Vl4 Vl5
<...output truncated...>
Router#
```

Enabling or Disabling PFC Features on an Interface

You can enable or disable the PFC QoS features implemented on the PFC for traffic from an interface (see the "PFC Marking and Policing" section on page 32-16). Disabling the PFC QoS features on an interface leaves the configuration intact. The **mls qos** interface command reenables any previously configured PFC QoS features. The **mls qos** interface command does not affect the port queueing configuration.

To enable or disable PFC features for traffic from an interface, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** {{*type*[1] *slot/port*} | {**port-channel** *number*}}	Selects the interface to configure.
Step 2	Router(config-if)# **mls qos**	Enables PFC QoS on the interface.
	Router(config-if)# **no mls qos**	Disables PFC QoS on the interface.
Step 3	Router(config-if)# **end**	Exits configuration interface.
Step 4	Router# **show mls qos**	Verifies the configuration.

[1] *type* = **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **ge-wan**, **pos**, or **atm**

This example shows how to disable PFC QoS on the VLAN 5 interface:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan 5
Router(config-if)# no mls qos
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos | begin QoS is disabled
  QoS is disabled on the following interfaces:
    Vl5
<...Output Truncated...>
Router#
```

Enabling VLAN-Based PFC QoS on Layer 2 LAN Ports

Note With DFCs installed, Supervisor Engine 2 does not support VLAN-based PFC QoS.

By default, PFC QoS uses policy maps attached to LAN ports. For ports configured as Layer 2 LAN ports with the **switchport** keyword, you can configure PFC QoS to use policy maps attached to a VLAN (see the "Attaching Policy Maps" section on page 32-21). Ports not configured with the **switchport** keyword are not associated with a VLAN.

To enable VLAN-based PFC QoS on a Layer 2 LAN port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{type[1] slot/port}	{port-channel number}}`	Selects the interface to configure.
Step 2	`Router(config-if)# mls qos vlan-based`	Enables VLAN-based PFC QoS on a Layer 2 LAN port.
	`Router(config-if)# no mls qos vlan-based`	Disables VLAN-based PFC QoS.
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show mls qos`	Verifies the configuration.

[1] *type* = **ethernet, fastethernet, gigabitethernet,** or **tengigabitethernet**

This example shows how to enable VLAN-based PFC QoS on Fast Ethernet port 5/42:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/42
Router(config-if)# mls qos vlan-based
Router(config-if)# end
```

This example shows how to verify the configuration:

```
Router# show mls qos | begin QoS is vlan-based
  QoS is vlan-based on the following interfaces:
    Fa5/42
<...Output Truncated...>
```

Note Configuring a Layer 2 LAN port for VLAN-based PFC QoS preserves the policy map port configuration. The **no mls qos vlan-based** port command reenables any previously configured port commands.

Configuring the Trust State of Ethernet LAN and OSM Ingress Ports

By default, all ingress ports are untrusted. You can configure the ingress port trust state on all Ethernet LAN ports except non-Gigabit Ethernet **1q4t/2q2t** ports (see the "Ingress LAN Port Features" section on page 32-12). You can configure the ingress port trust state on OSM ports (see the "Ingress OSM Port Features" section on page 32-11).

To configure the trust state of an ingress port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{type[1] slot/port} | {port-channel number}}`	Selects the interface to configure.
Step 2	`Router(config-if)# mls qos trust [dscp | ip-precedence | cos[2]]`	Configures the trust state of the port.
	`Router(config-if)# no mls qos trust`	Reverts to the default trust state (untrusted).
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show mls qos`	Verifies the configuration.

[1] *type* = **ethernet, fastethernet, gigabitethernet, tengigabitethernet, ge-wan, pos,** or **atm.**

[2] Not supported for **pos** or **atm** interface types.

When configuring the trust state of an ingress port, note the following:

- With no other keywords, the **mls qos trust** command is equivalent to **mls qos trust dscp**.
- The **mls qos trust cos** command enables receive-queue drop thresholds. To avoid dropping traffic because of inconsistent CoS values, configure ports with the **mls qos trust cos** command only when the received traffic is ISL or 802.1Q frames carrying CoS values that you know to be consistent with network policy.
- Use the **no mls qos trust** command to set the port state to untrusted.

This example shows how to configure Gigabit Ethernet port 1/1 with the **trust cos** keywords:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# mls qos trust cos
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/1 | include trust
  Trust state: trust COS
Router#
```

Configuring the Ingress LAN Port CoS Value

Note Whether or not PFC QoS uses the CoS value applied with the **mls qos cos** command depends on the trust state of the port and the trust state of the traffic received through the port. The **mls qos cos** command does not configure the trust state of the port or the trust state of the traffic received through the port. To use the CoS value applied with the **mls qos cos** command, configure the ingress port as trusted or configure a trust-CoS policy map that matches the ingress traffic.

You can configure the CoS value that PFC QoS assigns to untagged frames from ingress LAN ports configured as trusted and to all frames from ingress LAN ports configured as untrusted.

To configure the CoS value for an ingress LAN port, perform this task:

	Command	Purpose
Step 1	`Router(config)# `**`interface`**` {{`*`type`*[1]` `*`slot/port`*`} | {`**`port-channel`**` `*`number`*`}}`	Selects the interface to configure.
Step 2	`Router(config-if)# `**`mls qos cos`**` `*`default_cos`*	Configures the ingress LAN port CoS value.
	`Router(config-if)# `**`[no] mls qos cos`**` `*`default_cos`*	Reverts to the default port CoS value.
Step 3	`Router(config-if)# `**`end`**	Exits configuration mode.
Step 4	`Router# `**`show queueing interface {ethernet | fastethernet | gigabitethernet}`**` `*`slot/port`*	Verifies the configuration.

[1] *type* = **ethernet, fastethernet, gigabitethernet, or tengigabitethernet**

This example shows how to configure the CoS 5 as the default on Fast Ethernet port 5/24 and verify the configuration:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/24
Router(config-if)# mls qos cos 5
Router(config-if)# end
Router# show queueing interface fastethernet 5/24 | include Default COS
  Default COS is 5
Router#
```

Configuring LAN-Port Drop Threshold Percentages

These sections describe LAN-port drop-threshold configuration:

- Configuring Tail-Drop Threshold Percentages on 1q4t/2q2t LAN Ports, page 32-53
- Configuring 1q2t and 1p1q4t Standard Receive-Queue Tail-Drop Threshold Percentages, page 32-54
- Configuring Standard Queue WRED-Drop Thresholds, page 32-55

Note Enter the **show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** command to see the queue structure of a port.

Configuring Tail-Drop Threshold Percentages on 1q4t/2q2t LAN Ports

The receive- and transmit-queue drop thresholds have this relationship:

- Receive queue 1 (standard) threshold 1 = transmit queue 1 (standard low priority) threshold 1
- Receive queue 1 (standard) threshold 2 = transmit queue 1 (standard low priority) threshold 2
- Receive queue 1 (standard) threshold 3 = transmit queue 2 (standard high priority) threshold 1
- Receive queue 1 (standard) threshold 4 = transmit queue 2 (standard high priority) threshold 2

To configure tail-drop threshold percentages for the standard receive and transmit queues on **1q4t/2q2t** LAN ports (see the "Transmit Queues" section on page 32-21), perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {ethernet	fastethernet	gigabitethernet} slot/port`	Selects the interface to configure.
Step 2	`Router(config-if)# wrr-queue threshold queue_id thr1% thr2%`	Configures the receive- and transmit-queue tail-drop thresholds.
	`Router(config-if)# no wrr-queue threshold [queue_id]`	Reverts to the default receive- and transmit-queue tail-drop thresholds.
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show queueing interface {ethernet	fastethernet	gigabitethernet} slot/port`	Verifies the configuration.

When configuring the receive- and transmit-queue tail-drop thresholds, note the following:

- You must use the transmit queue and threshold numbers.
- The *queue_id* is 1 for the standard low-priority queue and 2 for the standard high-priority queue.
- The percentages range from 1 to 100. A value of 10 indicates a threshold when the buffer is 10-percent full.
- Always set threshold 2 to 100 percent.

This example shows how to configure receive queue 1/threshold 1 and transmit queue 1/threshold 1 for Gigabit Ethernet port 2/1:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 2/1
Router(config-if)# wrr-queue threshold 1 60 100
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 2/1
  Transmit queues [type = 2q2t]:

<...Output Truncated...>

queue tail-drop-thresholds
    --------------------------
    1     60[1] 100[2]
    2     40[1] 100[2]

<...Output Truncated...>
```

```
Receive queues [type = 1q4t]:

<...Output Truncated...>

queue tail-drop-thresholds
--------------------------
    1     60[1] 100[2] 40[3] 100[4]
<...Output Truncated...>
Router#
```

Note Receive-queue tail-drop thresholds are supported only on ingress Gigabit Ethernet LAN ports configured to trust CoS.

Configuring 1q2t and 1p1q4t Standard Receive-Queue Tail-Drop Threshold Percentages

Note Configure **1q4t** standard receive-queue tail-drop threshold percentages with the **wrr-queue threshold** command (see the "Configuring Tail-Drop Threshold Percentages on 1q4t/2q2t LAN Ports" section on page 32-53).

To configure tail-drop threshold percentages for the standard receive queues on a **1q2t** or **1p1q4t** ingress LAN port (see the "Receive Queues" section on page 32-13), perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** {**fastethernet** | **gigabitethernet**} *slot/port*	Selects the interface to configure.
Step 2	Router(config-if)# **rcv-queue threshold** *queue_id thr1% thr2%* [*thr3% thr4%*]	Configures the receive-queue tail-drop threshold percentages.
	Router(config-if)# **no rcv-queue threshold** [*queue_id*]	Reverts to the default receive-queue tail-drop threshold percentages.
Step 3	Router(config-if)# **end**	Exits configuration mode.
Step 4	Router# **show queueing interface** {**fastethernet** | **gigabitethernet**} *slot/port*	Verifies the configuration.

When configuring the receive-queue tail-drop threshold percentages, note the following:

- The *queue_id* is always 1.
- The percentages range from 1 to 100. A value of 10 indicates a threshold when the buffer is 10-percent full.
- On a **1q2t** ingress LAN port, always set threshold 2 to 100 percent.
- On a **1p1q4t** ingress LAN port, always set threshold 4 to 100 percent.

This example shows how to configure the receive-queue drop thresholds for Gigabit Ethernet port 1/1:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# rcv-queue threshold 1 60 75 85 100
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/1 | begin Receive queues
Receive queues [type = 1p1q4t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1          Standard             4
       2          Priority             1

  Trust state: trust COS

    queue tail-drop-thresholds
    --------------------------
    1     60[1] 75[2] 85[3] 100[4]
<...Output Truncated...>
Router#
```

Configuring Standard Queue WRED-Drop Thresholds

1p2q2t, **1p3q1t**, and **1p2q1t** ports have WRED-drop thresholds in their standard transmit queues.

1p1q8t ports have WRED-drop thresholds in their standard receive queue.

Note **1p3q1t** (transmit), **1p2q1t** (transmit), and **1p1q8t** (receive) ports also have nonconfigurable tail-drop thresholds (see the "1p3q1t Ports" section on page 32-23).

To configure the WRED-drop thresholds (see the "Transmit Queues" section on page 32-21), perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** *type*[1] *slot/port*	Selects the interface to configure.
Step 2	Router(config-if)# **wrr-queue random-detect min-threshold** *queue_id thr1%* [*thr2%* [*thr3% thr4% thr5% thr6% thr7% thr8%*]]	Configures the low WRED-drop thresholds.
	Router(config-if)# **no wrr-queue random-detect min-threshold** [*queue_id*]	Reverts to the default low WRED-drop thresholds.
Step 3	Router(config-if)# **wrr-queue random-detect max-threshold** *queue_id thr1%* [*thr2%* [*thr3% thr4% thr5% thr6% thr7% thr8%*]]]	Configures the high WRED-drop thresholds.
	Router(config-if)# **no wrr-queue random-detect max-threshold** [*queue_id*]	Reverts to the default high WRED-drop thresholds.
Step 4	Router(config-if)# **end**	Exits configuration mode.
Step 5	Router# **show queueing interface** *type*[1] *slot/port*	Verifies the configuration.

[1] *type* = **fastethernet, gigabitethernet, or tengigabitethernet**

When configuring the WRED-drop thresholds, note the following:

- Each threshold has a low- and a high-WRED value.
- WRED values are a percentage of the queue capacity (the range is from 1 to 100).
- The low-WRED value is the traffic level under which no traffic is dropped. The low-WRED value must be lower than the high-WRED value. Configure the low-WRED value with the **min-threshold** keyword.

The high-WRED value is the traffic level above which all traffic is dropped. Configure the high-WRED value with the **max-threshold** keyword.

Note Traffic in the queue between the low- and high-WRED values has an increasing chance of being dropped as the queue fills.

- When configuring **1p2q2t** ports, note the following:
  - Queue number 1 is the low-priority standard transmit queue
  - Queue number 2 is high priority standard transmit queue
  - Each queue has two thresholds.
- When configuring **1p3q1t** ports, note the following:
  - Queue number 1 is the low-priority standard transmit queue.
  - Queue number 2 is the medium priority standard transmit queue.
  - Queue number 3 is the high priority standard transmit queue.
  - Each queue has one threshold.
  - When you configure each standard transmit queue, the single percentage that you enter sets the threshold.
- When configuring **1p1q8t** ports, note the following:
  - Queue number 1 is the single standard receive queue.
  - When you configure the single standard receive queue, note the following:

    The first percentage that you enter sets the lowest-priority threshold.

    The second percentage that you enter sets the next highest-priority threshold.

    The eighth percentage that you enter sets the highest-priority threshold.
- When configuring **1p2q1t** ports, note the following:
  - Queue number 1 is the low-priority standard transmit queue
  - Queue number 2 is high priority standard transmit queue
  - When you configure each standard transmit queue, the single percentage that you enter sets the threshold.

This example shows how to configure the low-priority transmit queue high-WRED-drop thresholds for Gigabit Ethernet port 1/1:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# wrr-queue random-detect max-threshold 1 70 70
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/1 | begin Transmit queues
  Transmit queues [type = 1p2q2t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         WRR low             2
       2         WRR high            2
       3         Priority            1
    queue random-detect-max-thresholds
    ----------------------------------
      1     40[1]  70[2]
      2     40[1]  70[2]
<...Output Truncated...>
Router#
```

Enabling and Disabling WRED-Drop Thresholds

To enable or disable WRED-drop thresholds on **1p3q1t** or **1p2q1t** transmit queues or **1p1q8t** receive queues, perform this task:

	Command	Purpose
Step 1	`Router(config)# `**`interface`**` `*`type`*[1]` `*`slot/port`*	Selects the interface to configure.
Step 2	`Router(config-if)# `**`wrr-queue random-detect`**` `*`queue_id`*	Enables WRED-drop thresholds on queue 1, 2, or 3.
	`Router(config-if)# `**`no wrr-queue random-detect`**` [`*`queue_id`*`]`	Reverts to the default WRED-drop thresholds.
Step 3	`Router(config-if)# `**`end`**	Exits configuration mode.
Step 4	`Router# `**`show queueing interface`**` `*`type`*[1]` `*`slot/port`*	Verifies the configuration.

[1] *type* = **fastethernet** or **tengigabitethernet**

Mapping CoS Values to LAN-Port Drop Thresholds

These sections describe mapping CoS values to LAN-port drop thresholds:

- Mapping CoS Values to 1q4t/2q2t LAN Ports, page 32-57
- Mapping CoS Values on 1p1q4t/1p2q2t, 1p1q0t/1p3q1t, and 1p1q8t/1p2q1t LAN Ports, page 32-58

Mapping CoS Values to 1q4t/2q2t LAN Ports

Note Enter the **show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** command to see the queue structure of a port.

On **1q4t/2q2t** LAN ports, the receive- and transmit-queue tail-drop thresholds have this relationship:

- Receive queue 1 (standard) threshold 1 = transmit queue 1 (standard low priority) threshold 1
- Receive queue 1 (standard) threshold 2 = transmit queue 1 (standard low priority) threshold 2
- Receive queue 1 (standard) threshold 3 = transmit queue 2 (standard high priority) threshold 1
- Receive queue 1 (standard) threshold 4 = transmit queue 2 (standard high priority) threshold 2

To map CoS values to tail-drop thresholds, perform this task:

	Command	Purpose
Step 1	`Router(config)# `**`interface`**` `*`type`*[1]` `*`slot/port`*	Selects the interface to configure.
Step 2	`Router(config-if)# `**`wrr-queue cos-map`**` `*`transmit_queue_# threshold_# cos1`*` [`*`cos2`*` [`*`cos3`*` [`*`cos4`*` [`*`cos5`*` [`*`cos6`*` [`*`cos7`*` [`*`cos8`*`]]]]]]]`	Maps CoS values to a tail-drop threshold.
Step 3	`Router(config-if)# `**`no wrr-queue cos-map`**	Reverts to the default mapping.
Step 4	`Router(config-if)# `**`end`**	Exits configuration mode.
Step 5	`Router# `**`show queueing interface`**` `*`type`*[1]` `*`slot/port`*	Verifies the configuration.

[1] *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When mapping CoS values to a tail-drop threshold, note the following:

- Use the transmit queue and threshold numbers.
- Queue 1 is the low-priority standard transmit queue.
- Queue 2 is the high-priority standard transmit queue.
- There are two thresholds in each queue.
- Enter up to 8 CoS values to map to the threshold.

This example shows how to map the CoS values 0 and 1 to standard transmit queue 1/threshold 1 for Fast Ethernet port 5/36:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface fastethernet 5/36 | begin queue thresh cos-map
    queue thresh cos-map
    ---------------------------------------
    1      1      0 1
    1      2      2 3
    2      1      4 5
    2      2      6 7
<...Output Truncated...>
Router#
```

Mapping CoS Values on 1p1q4t/1p2q2t, 1p1q0t/1p3q1t, and 1p1q8t/1p2q1t LAN Ports

Note Enter the **show queueing interface** {**ethernet** | **fastethernet** | **gigabitethernet** | **tengigabitethernet**} *slot/port* | **include type** command to see the queue structure of a port.

These sections describe how to map CoS values:

- Mapping CoS Values to Standard Receive-Queue Tail-Drop Thresholds, page 32-59
- Mapping CoS Values to WRED-Drop Thresholds, page 32-59
- Mapping CoS Values to Strict-Priority Queues, page 32-61

Mapping CoS Values to Standard Receive-Queue Tail-Drop Thresholds

To map CoS values to the standard receive-queue tail-drop thresholds on **1q2t**, **1p1q4t**, and **1p1q0t** ingress LAN ports, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** {**fastethernet** | **gigabitethernet**} *slot/port*	Selects the interface to configure.
Step 2	Router(config-if)# **rcv-queue cos-map** *queue_# threshold_# cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	Maps CoS values to the standard receive queue tail-drop thresholds. The queue number is always 1.
	Router(config-if)# **no rcv-queue cos-map**	Reverts to the default mapping.
Step 3	Router(config-if)# **end**	Exits configuration mode.
Step 4	Router# **show queueing interface** {**fastethernet** | **gigabitethernet**} *slot/port*	Verifies the configuration.

This example shows how to map the CoS values 0 and 1 to threshold 1 in the standard receive queue for Gigabit Ethernet port 1/1:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# rcv-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/1
<...Output Truncated...>
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    1     3      4 5
    1     4      6 7
<...Output Truncated...>
Router#
```

Mapping CoS Values to WRED-Drop Thresholds

To map CoS values to WRED-drop thresholds, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** {**fastethernet** | **gigabitethernet**} *slot/port*	Selects the interface to configure.
Step 2	Router(config-if)# **wrr-queue cos-map** *transmit_queue_# threshold_# cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	Maps CoS values to a WRED-drop threshold.
	Router(config-if)# **no wrr-queue cos-map**	Reverts to the default mapping.
Step 3	Router(config-if)# **end**	Exits configuration mode.
Step 4	Router# **show queueing interface** {**fastethernet** | **gigabitethernet**} *slot/port*	Verifies the configuration.

When associating CoS values to a WRED-drop threshold, note the following:

- On **1p2q2t** egress LAN ports:
  - Queue 1 is the low-priority standard transmit queue.
  - Queue 2 is the high-priority standard transmit queue.
  - There are two WRED-drop thresholds in each queue. Threshold 1 is low-priority and threshold 2 is high-priority.
- On **1p3q1t** egress LAN ports:
  - Queue 1 is the low-priority standard transmit queue.
  - Queue 2 is the medium-priority standard transmit queue.
  - Queue 3 is the high-priority standard transmit queue.
  - Each queue has two thresholds. Threshold 0 is the nonconfigurable 100-percent tail-drop threshold. Threshold 1 the WRED-drop threshold (see the "Enabling and Disabling WRED-Drop Thresholds" section on page 32-57 and the "Configuring Standard Queue WRED-Drop Thresholds" section on page 32-55).
- On **1p1q8t** ingress LAN ports:
  - Queue 1 is the standard queue.
  - Queue 1 has nine thresholds. Threshold 0 is the nonconfigurable 100-percent tail-drop threshold. Thresholds 1 through 8 are the WRED-drop thresholds (see the "Enabling and Disabling WRED-Drop Thresholds" section on page 32-57 and the "Configuring Standard Queue WRED-Drop Thresholds" section on page 32-55).
- On **1p2q1t** egress LAN ports:
  - Queue 1 is the standard queue.
  - Queue 1 has two thresholds. Threshold 0 is the nonconfigurable 100-percent tail-drop threshold. Threshold 1 the WRED-drop threshold (see the "Enabling and Disabling WRED-Drop Thresholds" section on page 32-57 and the "Configuring Standard Queue WRED-Drop Thresholds" section on page 32-55).
- You can enter up to 8 CoS values to map to the threshold.

This example shows how to map the CoS values 0 and 1 to standard transmit queue 1/threshold 1 for Fast Ethernet port 5/36:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 5/36
Router(config-if)# wrr-queue cos-map 1 1 0 1
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface fastethernet 5/36 | begin queue thresh cos-map
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    2     1      4 5
    2     2      6 7
<...Output Truncated...>
Router#
```

Mapping CoS Values to Strict-Priority Queues

To map CoS values to the receive and transmit strict-priority queues on **1p1q4t/1p2q2t, 1p1q0t/1p3q1t** and **1p1q8t/1p2q1t** LAN ports, perform this task:

	Command	Purpose
Step 1	`Router(config)#` **`interface`** *`type`*[1] *`slot/port`*	Selects the interface to configure.
Step 2	`Router(config-if)#` **`priority-queue cos-map`** *`queue_# cos1`* `[`*`cos2`* `[`*`cos3`* `[`*`cos4`* `[`*`cos5`* `[`*`cos6`* `[`*`cos7`* `[`*`cos8`*`]]]]]]]`	Maps CoS values to the receive and transmit strict-priority queues.
	`Router(config-if)#` **`no priority-queue cos-map`**	Reverts to the default mapping.
Step 3	`Router(config-if)#` **`end`**	Exits configuration mode.
Step 4	`Router#` **`show queueing interface`** *`type`*[1] *`slot/port`*	Verifies the configuration.

[1] *type* = **fastethernet, gigabitethernet, or tengigabitethernet**

When mapping CoS values to the strict-priority queues, note the following:

- The queue number is always 1.
- You can enter up to 8 CoS values to map to the queue.

This example shows how to map CoS value 7 to the strict-priority queues on Gigabit Ethernet port 1/1:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/1
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/1
<...Output Truncated...>
Transmit queues [type = 1p2q2t]:
<...Output Truncated...>
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    2     1      4
    2     2      6
    3     1      5 7

  Receive queues [type = 1p1q4t]:
<...Output Truncated...>
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1
    1     2      2 3
    1     3      4
    1     4      6
    2     1      5 7
<...Output Truncated...>
Router#
```

Allocating Bandwidth Between LAN-Port Transmit Queues

The switch transmits frames from one standard queue at a time using a WRR algorithm. WRR uses the ratio between queue weight values to decide how much to transmit from one queue before switching to the other. The more the ratio favors a queue, the more transmit bandwidth is allocated to it.

To allocate bandwidth for an egress LAN port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface type[1] slot/port`	Selects the interface to configure.
Step 2	`Router(config-if)# wrr-queue bandwidth low_priority_queue_weight [medium_priority_queue_weight] high_priority_queue_weight`	Allocates bandwidth between standard transmit queues. The valid values for weight range from 1 to 255.
	`Router(config-if)# no wrr-queue bandwidth`	Reverts to the default bandwidth allocation.
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show queueing interface type[1] slot/port`	Verifies the configuration.

[1] *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to allocate a 3-to-1 bandwidth ratio for Gigabit Ethernet port 1/2:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# wrr-queue bandwidth 3 1
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/2 | include bandwidth
WRR bandwidth ratios:    3[queue 1]    1[queue 2]
Router#
```

Setting the Receive-Queue Size Ratio on a 1p1q0t or 1p1q8t Ingress LAN Ports

To set the size ratio between the strict-priority and standard receive queues on a **1p1q0t** or **1p1q8t** ingress LAN ports, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {fastethernet	tengigabitethernet} slot/port`	Selects the interface to configure.
Step 2	`Router(config-if)# rcv-queue queue-limit standard_queue_weight strict_priority_queue_weight`	Sets the size ratio between the strict-priority and standard receive queues.
	`Router(config-if)# no rcv-queue queue-limit`	Reverts to the default the size ratio.
Step 3	`Router(config-if)# end`	Exits configuration mode.
Step 4	`Router# show queueing interface {fastethernet	tengigabitethernet} slot/port`	Verifies the configuration.

When setting the receive-queue size ratio, note the following:

- The **rcv-queue queue-limit** command configures ports on a per-ASIC basis.
- Estimate the mix of strict priority-to-standard traffic on your network (for example, 80 percent standard traffic and 20 percent strict-priority traffic).
- Use the estimated percentages as queue weights.
- Valid values are from 1 to 100 percent, except on **1p1q8t** ingress LAN ports, where valid values for the strict priority queue are from 3 to 100 percent.

This example shows how to set the receive-queue size ratio for Fast Ethernet port 2/2:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 2/2
Router(config-if)# rcv-queue queue-limit 75 15
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface fastethernet 2/2 | include queue-limit
    queue-limit ratios:     75[queue 1]  15[queue 2]
Router#
```

Setting the LAN-Port Transmit-Queue Size Ratio

To set the transmit-queue size ratio on an egress LAN port, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** *type*[1] *slot/port*	Selects the interface to configure.
Step 2	Router(config-if)# **wrr-queue queue-limit** *low_priority_queue_weight* [*medium_priority_queue_weight*] *high_priority_queue_weight*	Sets the transmit-queue size ratio between transmit queues.
	Router(config-if)# **no wrr-queue queue-limit**	Reverts to the default transmit-queue size ratio.
Step 3	Router(config-if)# **end**	Exits configuration mode.
Step 4	Router# **show queueing interface** *type*[1] *slot/port*	Verifies the configuration.

[1] *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

When setting the transmit-queue size ratio between transmit queues, note the following:

- Estimate the mix of low priority-to-high priority traffic on your network (for example, 80 percent low-priority traffic and 20 percent high-priority traffic).
- On **1p2q2t** egress LAN ports, PFC QoS sets the strict-priority queue size equal to the high priority queue size.
- Use the estimated percentages as queue weights.
- Valid values are from 1 to 100 percent, except on **1p2q1t** egress LAN ports, where valid values for the high priority queue are from 5 to 100 percent.

This example shows how to set the transmit-queue size ratio for Gigabit Ethernet port 1/2:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 1/2
Router(config-if)# wrr-queue queue-limit 75 15
Router(config-if)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show queueing interface gigabitethernet 1/2 | include queue-limit
    queue-limit ratios:      75[queue 1]  25[queue 2]
Router#
```

Configuring DSCP Value Maps

These sections describe how DSCP values are mapped to other values:

- Mapping Received CoS Values to Internal DSCP Values, page 32-64
- Mapping Received IP Precedence Values to Internal DSCP Values, page 32-65
- Mapping Internal DSCP Values to Egress CoS Values, page 32-65
- Configuring DSCP Markdown Values, page 32-66

Mapping Received CoS Values to Internal DSCP Values

To configure the mapping of received CoS values to the DSCP value that PFC QoS uses internally on the PFC (see the "Internal DSCP Values" section on page 32-17), perform this task:

	Command	Purpose
Step 1	`Router(config)# mls qos map cos-dscp dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8`	Configures the received CoS to internal DSCP map. You must enter 8 DSCP values to which PFC QoS maps CoS values 0 through 7.
	`Router(config)# no mls qos map cos-dscp`	Reverts to the default map.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos maps`	Verifies the configuration.

This example shows how to configure the received CoS to internal DSCP map:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map cos-dscp 0 1 2 3 4 5 6 7
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos maps | begin Cos-dscp map
   Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     ----------------------------------
       dscp:   0  1  2  3  4  5  6  7
<...Output Truncated...>
Router#
```

Mapping Received IP Precedence Values to Internal DSCP Values

To configure the mapping of received IP precedence values to the DSCP value that PFC QoS uses internally on the PFC (see the "Internal DSCP Values" section on page 32-17), perform this task:

	Command	Purpose
Step 1	`Router(config)# mls qos map ip-prec-dscp dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8`	Configures the received IP precedence to internal DSCP map. You must enter 8 internal DSCP values to which PFC QoS maps received IP precedence values 0 through 7.
	`Router(config)# no mls qos map ip-prec-dscp`	Reverts to the default map.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos maps`	Verifies the configuration.

This example shows how to configure the received IP precedence to internal DSCP map:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map ip-prec-dscp 0 1 2 3 4 5 6 7
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos maps | begin IpPrecedence-dscp map
   IpPrecedence-dscp map:
     ipprec:   0  1  2  3  4  5  6  7
     ---------------------------------
       dscp:   0  1  2  3  4  5  6  7
<...Output Truncated...>
Router#
```

Mapping Internal DSCP Values to Egress CoS Values

To configure the mapping of the DSCP value that PFC QoS uses internally on the PFC to the CoS value used for egress LAN port scheduling and congestion avoidance (see the "Internal DSCP Values" section on page 32-17 and the "LAN Egress Port Features" section on page 32-21), perform this task:

	Command	Purpose
Step 1	`Router(config)# mls qos map dscp-cos dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]]] to cos_value`	Configures the internal DSCP to egress CoS map.
	`Router(config)# no mls qos map dscp-cos`	Reverts to the default map.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos maps`	Verifies the configuration.

When configuring the internal DSCP to egress CoS map, note the following:

- You can enter up to 8 DSCP values that PFC QoS maps to a CoS value.
- You can enter multiple commands to map additional DSCP values to a CoS value.
- You can enter a separate command for each CoS value.

This example shows how to configure internal DSCP values 0, 8, 16, 24, 32, 40, 48, and 54 to be mapped to egress CoS value 0:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map dscp-cos 0 8 16 24 32 40 48 54 to 0
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos map | begin Dscp-cos map
   Dscp-cos map:                                      (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     -------------------------------------
      0 :     00 00 00 00 00 00 00 00 00 01
      1 :     01 01 01 01 01 01 00 02 02 02
      2 :     02 02 02 02 00 03 03 03 03 03
      3 :     03 03 00 04 04 04 04 04 04 04
      4 :     00 05 05 05 05 05 05 05 00 06
      5 :     06 06 06 06 00 06 07 07 07 07
      6 :     07 07 07 07
<...Output Truncated...>
Router#
```

Note In the **Dscp-cos** display, the CoS values are shown in the body of the matrix; the first digit of the DSCP value is in the column labeled **d1** and the second digit is in the top row. In the example shown, DSCP values 41 through 47 all map to CoS 05.

Configuring DSCP Markdown Values

To configure the mapping of DSCP markdown values used by policers (see the "Policers" section on page 32-19), perform this task:

	Command	Purpose
Step 1	`Router(config)#` **`mls qos map policed-dscp {normal-burst	max-burst}`** *`dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7 [dscp8]]]]]]]`* **`to`** *`markdown_dscp`*	Configures a DSCP markdown map.
	`Router(config)#` **`no mls qos map policed-dscp {normal-burst	max-burst}`**	Reverts to the default map.
Step 2	`Router(config)#` **`end`**	Exits configuration mode.
Step 3	`Router#` **`show mls qos maps`**	Verifies the configuration.

When configuring a DSCP markdown map, note the following:

- You can enter the **normal-burst** keyword to configure the markdown map used by the **exceed-action policed-dscp-transmit** keywords.
- You can enter the **max-burst** keyword to configure the markdown map used by the **violate-action policed-dscp-transmit** keywords.

Note When you create a policer that does not use the **pir** keyword, and the *maximum_burst_bytes* parameter is equal to the *normal_burst_bytes* parameter (which occurs if you do not enter the *maximum_burst_bytes* parameter), the **exceed-action policed-dscp-transmit** keywords cause PFC QoS to mark traffic down as defined by the **policed-dscp max-burst** markdown map.

- To avoid out-of-sequence packets, configure the markdown maps so that conforming and nonconforming traffic uses the same queue.
- You can enter up to 8 DSCP values that map to a marked-down DSCP value.
- You can enter multiple commands to map additional DSCP values to a marked-down DSCP value.
- You can enter a separate command for each marked-down DSCP value.

Note Configure marked-down DSCP values that map to CoS values consistent with the markdown penalty (see the "Mapping Internal DSCP Values to Egress CoS Values" section on page 32-65).

This example shows how to map DSCP 1 to marked-down DSCP value 0:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mls qos map policed-dscp normal-burst 1 to 0
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show mls qos map
   Normal Burst Policed-dscp map:                               (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     -------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63

   Maximum Burst Policed-dscp map:                               (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     -------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    30 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
      5 :    50 51 52 53 54 55 56 57 58 59
      6 :    60 61 62 63
<...Output Truncated...>
Router#
```

Note In the **Policed-dscp** displays, the marked-down DSCP values are shown in the body of the matrix; the first digit of the original DSCP value is in the column labeled **d1** and the second digit is in the top row. In the example shown, DSCP 41 maps to DSCP 41.

Configuring PFC QoS Statistics Data Export

Note Release 12.1(11b)E and later releases support PFC QoS statistics data export.

These sections describe how to configure PFC QoS statistics data export:

- Enabling PFC QoS Statistics Data Export Globally, page 32-68
- Enabling PFC QoS Statistics Data Export for a Port, page 32-69
- Enabling PFC QoS Statistics Data Export for a Named Aggregate Policer, page 32-70
- Enabling PFC QoS Statistics Data Export for a Class Map, page 32-71
- Setting the PFC QoS Statistics Data Export Time Interval, page 32-72
- Configuring PFC QoS Statistics Data Export Destination Host and UDP Port, page 32-73
- Setting the PFC QoS Statistics Data Export Field Delimiter, page 32-75

Enabling PFC QoS Statistics Data Export Globally

To enable PFC QoS statistics data export globally, perform this task:

	Command	Purpose
Step 1	`Router(config)# mls qos statistics-export`	Enables PFC QoS statistics data export globally.
	`Router(config)# no mls qos statistics-export`	Disables PFC QoS statistics data export globally.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos statistics-export info`	Verifies the configuration.

This example shows how to enable PFC QoS statistics data export globally and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export
Router(config)# end
% Warning: Export destination not set.
% Use 'mls qos statistics-export destination' command to configure the export destination
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured
Router#
```

Note You must enable PFC QoS statistics data export globally for other PFC QoS statistics data export configuration to take effect.

Enabling PFC QoS Statistics Data Export for a Port

To enable PFC QoS statistics data export for a port, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface type[1] slot/port`	Selects the interface to configure.
Step 2	`Router(config-if)# mls qos statistics-export`	Enables PFC QoS statistics data export for the port.
	`Router(config-if)# no mls qos statistics-export`	Disables PFC QoS statistics data export for the port.
Step 3	`Router(config)# end`	Exits configuration mode.
Step 4	`Router# show mls qos statistics-export info`	Verifies the configuration.

[1] *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to enable PFC QoS statistics data export on FastEthernet port 5/24 and verify the configuration:

```
Router# configure terminal
Router(config)# interface fastethernet 5/24
Router(config-if)# mls qos statistics-export
Router(config-if)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24
Router#
```

When enabled on a port, PFC QoS statistics data export contains the following fields, separated by the delimiter character:

- Export type ("1" for a port)
- Slot/port
- Number of ingress packets
- Number of ingress bytes
- Number of egress packets
- Number of egress bytes
- Time stamp

Enabling PFC QoS Statistics Data Export for a Named Aggregate Policer

To enable PFC QoS statistics data export for a named aggregate policer, perform this task:

	Command	Purpose
Step 1	`Router(config)# mls qos statistics-export aggregate-policer aggregate_policer_name`	Enables PFC QoS statistics data export for a named aggregate policer.
	`Router(config)# no mls qos statistics-export aggregate-policer aggregate_policer_name`	Disables PFC QoS statistics data export for a named aggregate policer.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos statistics-export info`	Verifies the configuration.

This example shows how to enable PFC QoS statistics data export for an aggregate policer named aggr1M and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export aggregate-policer aggr1M
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M
Router#
```

When enabled for a named aggregate policer, PFC QoS statistics data export contains the following fields, separated by the delimiter character:

- Export type ("3" for an aggregate policer)
- Aggregate policer name
- Direction ("in")
- PFC or DFC slot number
- Number of in-profile packets
- Number of packets that exceed the CIR
- Number of packets that exceed the PIR
- Time stamp

Enabling PFC QoS Statistics Data Export for a Class Map

To enable PFC QoS statistics data export for a class map, perform this task:

	Command	Purpose
Step 1	Router(config)# **mls qos statistics-export class-map** *classmap_name*	Enables PFC QoS statistics data export for a class map.
	Router(config)# **no mls qos statistics-export class-map** *classmap_name*	Disables PFC QoS statistics data export for a class map.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show mls qos statistics-export info**	Verifies the configuration.

This example shows how to enable PFC QoS statistics data export for a class map named class3 and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export class-map class3
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 300 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
---------------------------------------------------------------
class3
Router#
```

When enabled for a class map, PFC QoS statistics data export contains the following fields, separated by the delimiter character:

- For data from a physical port:
  - Export type (“4” for a classmap and port)
  - Class map name
  - Direction (“in”)
  - Slot/port
  - Number of in-profile packets
  - Number of packets that exceed the CIR
  - Number of packets that exceed the PIR
  - Time stamp

- For data from a VLAN interface:
  - Export type ("5" for a class map and VLAN)
  - Classmap name
  - Direction ("in")
  - PFC or DFC slot number
  - VLAN ID
  - Number of in-profile packets
  - Number of packets that exceed the CIR
  - Number of packets that exceed the PIR
  - Time stamp
- For data from a port channel interface:
  - Export type ("6" for a class map and port-channel)
  - Class map name
  - Direction ("in")
  - PFC or DFC slot number
  - Port channel ID
  - Number of in-profile packets
  - Number of packets that exceed the CIR
  - Number of packets that exceed the PIR
  - Time stamp

Setting the PFC QoS Statistics Data Export Time Interval

To set the time interval for the PFC QoS statistics data export, perform this task:

	Command	Purpose
Step 1	Router(config)# **mls qos statistics-export interval** *interval_in_seconds*	Sets the time interval for the PFC QoS statistics data export. **Note** The interval needs to be short enough to avoid counter wraparound with the activity in your configuration, but because exporting PFC QoS statistic creates a significant load on the switch, be careful when decreasing the interval.
	Router(config)# **no mls qos statistics-export interval** *interval_in_seconds*	Reverts to the default time interval for the PFC QoS statistics data export.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show mls qos statistics-export info**	Verifies the configuration.

This example shows how to set the PFC QoS statistics data export interval and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export interval 250
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : |
Export Destination : Not configured

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
---------------------------------------------------------------
class3
Router#
```

Configuring PFC QoS Statistics Data Export Destination Host and UDP Port

To configure the PFC QoS statistics data export destination host and UDP port number, perform this task:

	Command	Purpose
Step 1	`Router(config)# mls qos statistics-export destination {host_name | host_ip_address} {port port_number | syslog [facility facility_name] [severity severity_value]}`	Configures the PFC QoS statistics data export destination host and UDP port number.
	`Router(config)# no mls qos statistics-export destination`	Clears configured values.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos statistics-export info`	Verifies the configuration.

Note When the PFC QoS data export destination is a syslog server, the exported data is prefaced with a syslog header.

Table 32-3 lists the supported PFC QoS data export facility and severity parameter values.

Table 32-3 Supported PFC QoS Data Export Facility Parameter Values

Name	Definition	Name	Definition
kern	kernel messages	cron	cron/at subsystem
user	random user-level messages	local0	reserved for local use
mail	mail system	local1	reserved for local use

Table 32-3 Supported PFC QoS Data Export Facility Parameter Values (continued)

Name	Definition	Name	Definition
daemon	system daemons	local2	reserved for local use
auth	security/authentication messages	local3	reserved for local use
syslog	internal syslogd messages	local4	reserved for local use
lpr	line printer subsytem	local5	reserved for local use
news	netnews subsytem	local6	reserved for local use
uucp	uucp subsystem	local7	reserved for local use

Table 32-4 lists the supported PFC QoS data export severity parameter values.

Table 32-4 Supported PFC QoS Data Export Severity Parameter Values

Severity Parameter		
Name	**Number**	**Definition**
emerg	0	system is unusable
alert	1	action must be taken immediately
crit	2	critical conditions
err	3	error conditions
warning	4	warning conditions
notice	5	normal but significant condition
info	6	informational
debug	7	debug-level messages

This example shows how to configure 172.20.52.3 as the destination host and syslog as the UDP port number and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export destination 172.20.52.3 syslog
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : |
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
---------------------------------------------------------------
class3
```

Setting the PFC QoS Statistics Data Export Field Delimiter

To set the PFC QoS statistics data export field delimiter, perform this task:

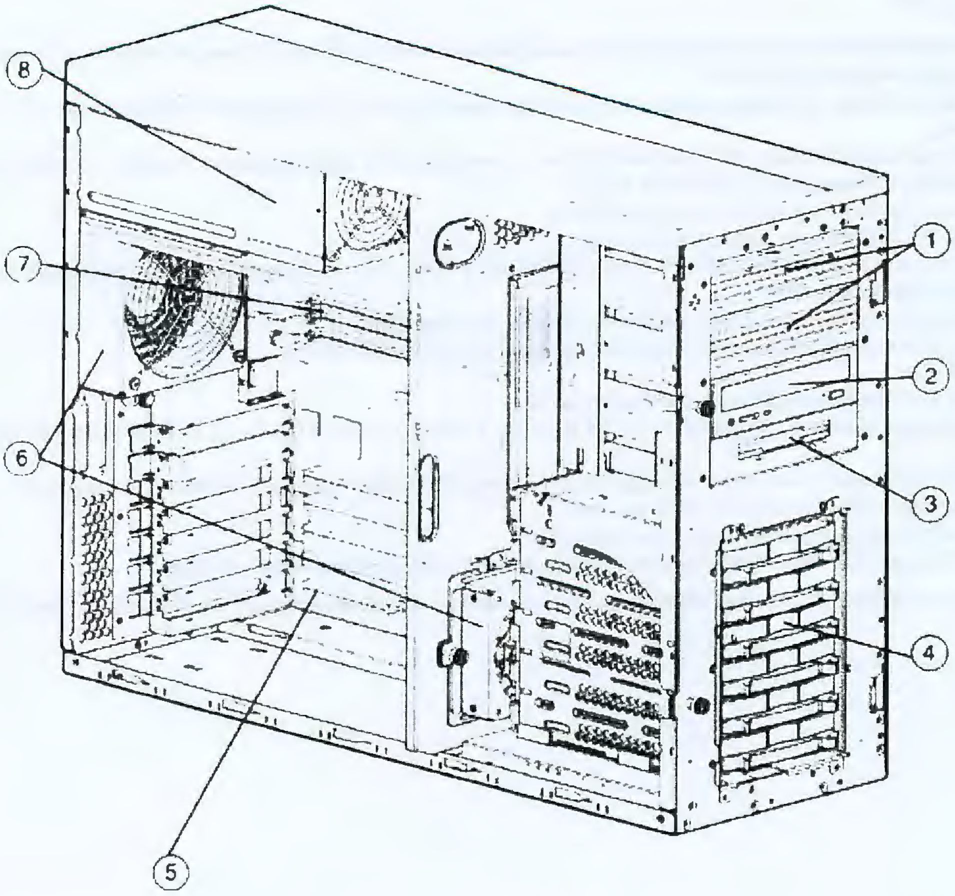
	Command	Purpose
Step 1	`Router(config)# mls qos statistics-export delimiter delimiter_character`	Sets the PFC QoS statistics data export field delimiter.
	`Router(config)# no mls qos statistics-export delimiter`	Reverts to the default PFC QoS statistics data export field delimiter
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show mls qos statistics-export info`	Verifies the configuration.

This example shows how to set the PFC QoS statistics data export field delimiter and verify the configuration:

```
Router# configure terminal
Router(config)# mls qos statistics-export delimiter ,
Router(config)# end
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : ,
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
---------------------------------------------------------------
class3
```

Apêndice FC

Overview



1. Two Removable Media Bays
2. 48X Max IDE (ATAPI) CD-ROM Drive
3. 1.44 Floppy Drive
4. Six 1" Hot Plug Drive Bays
5. Five expansion slots(four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI)
6. System fan
7. DIMM sockets for up to 8GB of memory, optionally interleaved
8. Optional 2nd Power Supply for hot-pluggable 1+1 redundancy

What's New

- Now available with Intel®Xeon 2.8 GHz Processors with 533MHz system bus.

Overview

At A Glance

- The ProLiant ML350 G3 is an expandable rack or tower platform delivering affordable 2-way performance and essential availability to corporate workgroups and growing businesses
- Intel Xeon 2.4 GHz or 2.8 GHz processors (dual processor capability) with 512-KB level 2 cache standard (full speed) and Hyper-Threading Technology
- ServerWorks Grand Champion LE Chipset with 533-MHz Front Side Bus for 2.8GHz processor models or 400-MHz FSB for models < 2.8 GHz
- Integrated Dual Channel Wide Ultra3 SCSI Adapter
- Smart Array Controller (standard in Array Models only)
- NC7760 PCI Gigabit Server Adapter (embedded)
- 512MB of 2-way interleaving capable PC2100 DDR SDRAM, with Advanced ECC capabilities (Array models only; 256MB standard on other models): Expandable to 8GB
- Flexible memory configurations allow interleaving (2x1) or non-interleaving
- Five available expansion slots: four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI
- Two USB ports
- Standard 6 x 1" Wide Ultra320 ready Hot Plug Drive Cage
- Internal storage capacity of up to 880GB (6 x 146.8 GB 1"), 1.174-TB (2 x 146.8 GB 1" + 6 x 146.8 GB 1") with optional 2-bay hot plug drive cage option
- 500W Hot-Pluggable Power Supply (standard) and an optional 500W Hot-Pluggable Redundant Power Supply (1+ 1) available
- Tool-free entry to chassis and access to components
- RBSU (ROM based setup utility) support, redundant ROM
- Insight Manager, SmartStart, ROM-based BIOS Setup Utility, and Automatic Server Recovery (ASR-2)
- Protected by HP Services, including a three-year, next business day, on-site, limited global warranty and extended Pre-Failure Warranty.

Standard Features

Processor *One of the following depending on Model:*	Intel Xeon Processor 2.8 GHz/533-512KB Intel Xeon Processor 2.4 GHz/400-512KB
Cache Memory	Integrated 512-KB Level 2 cache (full speed)
Upgradability	Upgradable to dual processing
Chipset	ServerWorks Grand Champion LE Chipset with 400-MHz or 533-MHz Front Side Bus (model dependent) NOTE: For more information regarding ServerWorks, please see the following URL. http://www.serverworks.com/products/overview.html NOTE: This Web site is available in English only.

Memory
(One of the following depending on model)

2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advanced ECC capabilities

Standard (Non-Array Models)	256MB
Standard (Array Models)	512MB
Maximum	8 GB

Network Controller

NC7760 Gigabit Server Adapter (embedded)

Expansion Slots

I/O (5 Total, 5 Available)		PCI Voltage:
64-bit/100MHz, PCI	4 (4 available) (Array model has 3 available)	3.3 Volt or universal cards
32-bit/33MHz, PCI	1 (1 available)	5 Volt or universal cards

Storage Controller

Integrated Dual Channel Wide Ultra3 SCSI Adapter
Smart Array 641 Controller (2.8 GHz Array Models Only)

Storage

Diskette Drives	1.44 MB
CD-ROM	48x IDE (ATAPI) CD-ROM Drive
Hard Drives	None
Maximum Internal Storage	1.174 TB GB (6 x 146.8 GB 1" with standard internal hot plug drive cage + (2 x 146.8 GB 1") with optional ML3xx Two Bay Hot Plug SCSI Drive Cage)
External Storage	Two external SCSI knockouts available, optional ProLiant ML350 Internal to External SCSI Cable Option Kit required ● HD68 Internal to External SCSI Cable Option Kit PN 159547-B22 ● VHDCI Internal to External SCSI Cable Option Kit PN 333370-B21

Standard Features

Interfaces	Parallel	1
	Serial	1
	Pointing Device (Mouse)	1
	Graphics	1
	Keyboard	1
	Network RJ-45	1
	USB	2 NOTE: Please see the following URL for additional information regarding USB support: http://www.compaq.com/products/servers/platforms/usb-support.html NOTE: This Web site is available in English only.
	External SCSI knockouts	2
Graphics	Integrated ATI RAGE XL Video Controller with 8-MB SDRAM Video Memory	
Form Factor	Tower or rack (5U) NOTE: Rack models (and rack conversion kit) support: ● Square hole racks from 27" - 32" deep (including Compaq/HP 7000, 9000, 10000 and H9 series) ● Square or round hole racks, from 24" - 35" deep (including HP Rack System /E and HP Systems, with an adjustment) ● Telco racks with 3rd part option kit from Rack Solutions http://www.racksolutions.com/compaq/products.htm NOTE: This Web site is available in English only.	

ProLiant Essentials Foundation Pack Software

Insight Manager 7

Insight Manager 7 helps maximize system uptime and performance and reduces the cost of maintaining the IT infrastructure by providing proactive notification of problems before those problems result in costly downtime and reduced productivity. Insight Manager 7 is easy to set up and provides rapid access to detailed fault and performance information gathered by the Management Agents. One-click-access to the Remote Insight Lights Out Edition II board allows systems administrators to take full graphical control of ProLiant servers in remote locations or lights-out data centers. Finally, Insight Manager 7 in concert with the Version Control Agents and Version Control Repository Manager enables systems administrators to version manage and update system software across groups of ProLiant servers.

Management Agents

The Management Agents form the foundation for HP's Intelligent Manageability strategy. They provide direct, browser-based access to in-depth instrumentation built into HP servers, workstations, desktops, and portables, and send alerts to Insight Manager 7 and other enterprise management applications in case of subsystem or environmental failures. For additional information about the Management Agents and other management products from HP, please visit the management Web site at http://www.hp.com/servers/manage

SmartStart

SmartStart is a tool that simplifies server setup, providing a rapid way to deploy reliable and consistent server configurations. For more information, please visit the SmartStart website at http://www.hp.com/servers/manage.
SmartStart version supported (minimum): SmartStart 5.50

ActiveUpdate

ActiveUpdate is a web-based application that keeps IT managers directly connected to HP for proactive notification and delivery of the latest software updates.

ROMPaq, support software, and configurotion utilities

The latest software, drivers, and firmware fully optimized and tested for your ProLiant server and options.

Survey Utility and diagnostics utilities

The most advanced configuration analysis, reporting and troubleshooting utilities used by HP and at your fingertips.

Optional Proliant Essentials Value Packs

Optional software offerings that selectively extend the functionality of an Adaptive Infrastructure to address specific business problems and needs:

- Rapid Deployment Pack – an automated solution for multi-server deployment and provisioning, enabling companies to quickly and easily adapt to changing business demands.
- Workload Management Pack – provides easier management of complex environments, improving overall server utilization and enabling Windows 2000 customers for the first time to confidently deploy multiple applications on a single multiprocessor ProLiant Server.
- Performance Management Pack – a performance management solution that identifies and explains hardware performance bottlenecks on ProLiant servers and attached options enabling users to better utilize their valuable resources.

NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Value Packs. Refer to http://www.hp.com/servers/proliantessentials or the various ProLiant Essentials Value Pack product QuickSpecs for more information.
NOTE: For more information regarding ProLiant Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentials
NOTE: These Web sites are available in English only

Industry Standard Compliance

ACPI V1.0B Compliant
PCI 2.2 Compliant
PXE Support
WOL Support
PCI-X 1.0 Compliant
Novell Certified
Microsoft Logo certifications

Standard Features

Manageability	Insight Monoger 7 Redundont ROM System Firmware Update ROMPoq Remote Insight Lights-Out Edition II (optional) ProLiant RBSU (ROM-Bosed Setup Utility) Automatic Server Recovery-2 (ASR-2) Drive Parameter Tracking (with Smart Array Controller) Dynamic Sector Repairing (with Smart Arroy Controller) Pre-Failure Warranty (covers processors, memory and hard drives)
Security	Power-on password Setup password Diskette boot control Porallel and serial interface control Disk configuration lock Power switch security
Server Power Cords	One Lowline NEMA power cord and one Highline IEC Power cord ship standard Tower models ship with standard country specific power cords. Rack models ship with IEC cables. Depending on the country, some also ship with country specific power cords Redundant power supply options ship with country specific power cords with the exception of the -B21 Rack SKU which ships with an IEC cable only.
Power Supply	500 Watts, Power Factor Correction (PFC), Hot Plug 100 to 240 VAC Rated Input Voltage (Auto-sensing), CE Mark Compliant Optional 2nd Power Supply for hot-pluggable 1 + 1 redundancy.
System Fans	2 fans ship standard, 2 fans total supported (does not include power supply fans)
Required Cabling	For required cabling information, refer to the HP Web site at http://www.hp.com/servers/proliantML350 NOTE: This Web site is available in English only.
OS Support	Microsoft Windows NT® Server 4.0 and Terminal Server 4.0 Microsoft BackOffice Small Business Server 2000 Microsoft Windows 2000 Server and Advanced Server Windows Server 2003 Novell NetWare 5.1, 6.0 Novell NetWore Small Business Suite 6.0 SCO OpenServer 5.0.6a SCO OpenUnix 8 SCO UnixWare 7.1.1 IBM OS/2 Warp Server for e-business LINUX (Red Hat, 2.1 Advanced Server, Red Hat 8.0 and Red Hat 7.3, SuSE, SLES7, UnitedLinux 1.0) NOTE: For a more complete and up-to date listing of supported OSs and versions, please visit our OS Support Matrix at: ftp://ftp.compaq.com/pub/products/servers/os-support-matrix-310.pdf NOTE: Optional hardware may be required to support some operating systems. NOTE: For an up-to-date listing of the latest drivers available for the ProLiant ML350, please see. http://www.compaq.com/support/files/server/us/index.html NOTE: These Web sites are available in English only.

Rack Airflow Requirements

- Rack 9000 and 10000 series Cabinets
  The increasing power of new high-performance processor technology requires increased cooling efficiency for rack-mounted servers. The 9000 and 10000 Series Racks provide enhanced airflow for maximum cooling, allowing these racks to be fully loaded with servers using the latest processors.

- Rack 7000 series Cabinets
  When installing a server with processors running at speeds of 550 MHz or greater in Rack 7000 series racks with glass doors (165753-001 (42U), and 163747-001 (22U)), the new processor technology requires the installation of HP's new High Airflow Rack Door Inserts (327281-B21 (42U), 327281-B22 (42U 6 pack), or 157847-B21 (22U)) to promote enhanced airflow for maximum cooling.

CAUTION: If a third-party rack is used, observe the following additional requirements to ensure adequate airflow and to prevent damage to the equipment:

- Front and rear doors: If your 42U server rack includes closing front and rear doors, you must allow 830 square inches (5,350 sq cm) of hole evenly distributed from top to bottom to permit adequate airflow (equivalent to the required 64 percent open area for ventilation).
- Side. The clearance between the installed rack component and the side panels of the rack must be a minimum of 2.75 inches (7 cm).

CAUTION: Always use blanking panels to fill all remaining empty front panel U-spaces in the rack. This arrangement ensures proper airflow. Using a rack without blanking panels results in improper cooling that can lead to thermal damage.

NOTE: For additional information, refer to the Setup and Installation Guide or the Documentation CD provided with the server, or to the server documentation located in the Support section of the following URL:
http://www5.hp.com/servers/proliantml350
NOTE: This Web site is available in English only.

Installation of Server into Telco Racks

ML350 G3 rack model support: Support for all 2-post Telco racks requires the use of the rack kit and an additional option kit from Rack Solutions. http://www.racksolutions.com/compaq
NOTE: This Web site is available in English only.

HP Factory Express Capabilities

HP Factory Express gives you the flexibility to choose from a full menu of factory capabilities all in one manufacturing facility, in one process, with one touch giving you full control and access to HP's World class manufacturing facility anytime. This approach provides you the speed to deploy your IT needs, with total quality assurance, reliability, and predictability to lower your total cost of ownership by letting HP install, rack, and customize your software and hardware options for you.

Standard Features

Service and Support

HP Services provides a three-year, limited warranty, including Pre-Failure Warranty (coverage of hard drives, memory and processors) fully supported by a worldwide network of resellers and service providers and lifetime toll-free 7 x 24 hardware technical phone support. In addition, available service offerings include:
NOTE: Limited Warranty includes 3 year Parts, 3 year Labor, 3-year on-site support.

A full range of HP Care Pack packaged hardware and software services:

- Installation and start up
- Extended coverage hours and enhanced response times
- System management and performance services
- Availability and recovery services

NOTE: For more infomation, visit http://www.hp.com/services/carepack.

Please see the following URL regarding Warranty Information For Your HP Products
http://www.compaq.com/support/warranty/upgrades/web_statements/176738.html

For additional information regarding Worldwide Limited Warranty and Technical Support, please see the following URL:
ftp://ftp.compaq.com/pub/supportinformation/ejourney/176738.pdf
NOTE: These Web sites are available in English only

NOTE: Certain restrictions and exclusions apply. Consult the Customer Support Center at 1-800-345-1518 for detai

Models

ML350T03 X2.8-512KB/533, 256MB *311523-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)
ML350R03 X2.8-512KB/533, 256MB *311524-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)
ML350T03 X2.8-512KB/533, 512MB Array *311525-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)
ML350R03 X2.8-512KB/533, 512MB Array *311526-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB of Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

Models

ML350T03 X2.4-512KB/400, 256MB *269786-001*	Processor(s)	(1) Intel Xeon Processor 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)

ML350R03 X2.4-512KB/400, 256MB *269787-001*	Processor(s)	(1) Xeon 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drives & drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

Options

ProLiant ML350 G3 Unique Options	Hot Plug Redundant Power Supply Option Kit	283655-001
	Hot Plug Redundant Power Supply Option Kit (cable) NOTE: PN 283655-B21 SKU contains the 2nd power supply with an IEC power cable. Only purchase if connecting to PDU/UPS that supports IEC cables. All other SKUs contain country specific power cables.	283655-B21
	Intel Xeon 2.80 GHz-512KB Processor Option Kit NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiant ML350 G3 systems with 533 MHz front side bus only. This kit cannot be used in 400 MHz front side bus systems such as those with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	314763-B21
	Intel Xeon 2.40 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 257913-B21) supports the ProLiant ML350 G3 servers.	257913-B21
	Intel Xeon 2.20 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 283702-B21) supports the ProLiant ML350 G3 servers.	283702-B21
	Intel Xeon 2.0 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 283701-B21) supports the ProLiant ML350 G3 servers.	283701-B21
	ProLiant ML350 G3 Tower to Rack Conversion Kit (CPQ brand)	290683-B21
ProLiant Essentials Value Pack Software	Rapid Deployment Pack, 1 User, V1.x NOTE: This license allows 1 server to be managed and deployed via the Deployment Server.	267196-B21
	Rapid Deployment Pack, 10 Users, V1.x NOTE: This license allows 10 servers to be managed and deployed via the Deployment Server.	269817-B21
	Flexible Quantity License Kit	302127-B21
	License-Only - for use with a Master License Agreement	302128-B21
	ProLiant Essentials Workload Management Pack 2.0 (Featuring Compaq Resource Partitioning Manager version 2.0)	303284-B21
	ProLiant Essentials Performance Management Pack Flexible License	306697-B21
	NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Value Packs. Refer to http://www.hp.com/servers/proliantessentials or the various ProLiant Essentials Value Pack product QuickSpecs for more information. NOTE: For more information regarding ProLiant Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentials NOTE: These Web sites are available in English only.	
HP NetServer Transition Services	HP NetServer to ProLiant integration and assessment service NOTE: HP identifies current levels of NetServer support, services, and management. This service helps maximize customer's ability to add ProLiant platforms into their current environment.	304164-002
	HP TopTools to Insight Manager 7 installation and startup service NOTE: Provides on-site review, installation and configuration services for Insight Manager 7. HP will also re-create, as closely as possible, the views and reports from the customer's current TopTools configuration. This service assures a smooth transition to the ProLiant Essentials software.	304163-002
	HP NetServer to ProLiant Essentials Rapid Deployment Pack installation and startup service NOTE: Install and configure Rapid Deployment Pack in a test environment, then deploy a server image to a maximum of 250 systems in the production environment. This service helps to assure successful system deployment.	304162-002

Options

Processors	**Intel Xeon 2.80 GHz-512KB Processor Option Kit**	314763-B21
	NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiant ML350 G3 systems with 533 MHz front side bus only. This kit cannot be used in 400 MHz front side bus systems such as thhose with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	
	Intel Xeon 2.40 GHz-512KB Processor Option Kit	257913-B21
	NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 257913-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	
	Intel Xeon 2.20 GHz-512KB Processor Option Kit	283702-B21
	NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283702-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	
	Intel Xeon 2.0 GHz-512KB Processor Option Kit	283701-B21
	NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283701-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	
Memory (DIMMs)	NOTE: The ML350 G3 supports both interleaved and non-interleaved memory configurations. Base models ship standard with one 256MB DIMM or one 512MB DIMM (Array models). For best performance automatically invoke interleaving by populating memory in identical pairs. If 1GB of total memory is desired add three 256MB DIMMs to the base configuration. If 1.5GB of memory is desired add one 256MB DIMM (to pair with the standard DIMM) and two 512MB DIMMs. Interleaving and installation of memory in pairs is not required. Add any combination of memory DIMMs below to operate in non-interleaved mode. NOTE: Each SDRAM Memory kit contains one (1) DIMM.	
	128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
	256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21
	512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21
	1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
	2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21
Internal Storage	**ML3xx Two Bay Hot Plug SCSI Drive Cage**	244059-B21
	NOTE: The drive cage option kit (PN 244059-B21) has one 1" drive bay and one 1 6' drive bay. It installs in two available removable media bays.	
Optical Drives	**16X DVD-ROM Drive Option Kit (Carbon)**	217053-B21
	CD-RW/DVD-ROM 48X Combo Drive Option Kit	3313[illegible]1
Hard Drives	*Ultra320 – Universal Hot Plug*	
	146.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286716-B22
	72.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286714-B22
	36.4-GB 10,000 rpm U320 Universal Hard Drive (1")	286713-B22
	72.8-GB 15,000 rpm U320 Universal Hard Drive (1")	286778-B22
	36.4-GB 15,000 rpm U320 Universal Hard Drive (1")	286776-B22
	18.2-GB 15,000 rpm U320 Universal Hard Drive (1")	286775-B22
	NOTE: All U320 Universal Hard Drives are backward compatible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates	
	NOTE. Please see the Wide Ultra320 Universal Hot Plug QuickSpecs for additional technical information on the hard drives Support details please see the following http www5 compaq com prod ts/quicksp [illegible]	

Options

Storage Controllers	Smart Array 6402/128 Controller	273915-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Compaq RAID LC2 Controller	188044-B21
	Smart Array 532 Controller	225338-B21
	Smart Array 5302/128 Controller	283552-B21
	Smart Array 5304/256 Controller	283551-B21
	Smart Array 5312 Controller	238633-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Ultra3 Channel Expansion Module for Smart Array 5300 Controller	153507-B21
	128-MB Cache Module for Smart Array 5302 Controller	153506-B21
	RAID ADG Upgrade for Smart Array 5302	288601-B21
	256-MB Battery Backed Cache Module NOTE: This 256-MB Battery Backed Cache Module supports the Smart Array 5300 series controllers, MSA 1000 and the Smart Array Cluster Storage.	254786-B21
	256MB Cache Upgrade for SA-6402 NOTE: This 256-MB Battery-Backed Cache Module upgrade kit supports the Smart Array 6400 series controller only.	273913-B21
	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS	284688-B21
	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter	268351-B21

NOTE: Please see the following Controller or SCSI Adapter QuickSpecs for Technical Specifications such as PCI Bus, PCI Peak Data Transfer Rate, SCSI Protocols supported, SCSI Peak Data Transfer Rate, Channels, SCSI Ports, Drives supported, Cache, RAID support, and additional information:

http://www5.compaq.com/products/quickspecs/10652_na/10652_na.HTML
(RAID LC2)
http://www5.compaq.com/products/quickspecs/10851_na/10851_na.HTML
(Smart Array 532)
http://www5.compaq.com/products/quickspecs/10640_na/10640_na.HTML
(Smart Array 5300 Series)
http://www5.compaq.com/products/quickspecs/11328_na/11328_na.HTML
(Smart Array 5312)
http://www5.compaq.com/products/quickspecs/11587_na/11587_na.HTML
(Smart Array 6402)
http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML
(Smart Array 641)
http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML
(Smart Array 642)
http://www5.compaq.com/products/quickspecs/10429_na/10429_na.HTML
(SCSI Adapter)
http://www5.compaq.com/products/quickspecs/11555_nav/11555_na.HTML
(U320 Adapter)

Wireless HAP Solution	Compaq WL410 Wireless SMB Access Point	191811-001

Options

Communications	NC3123 Fast Ethernet NIC PCI 10/100 WOL and PXE	174830-B21
	NC3134 Fast Ethernet NIC 64 PCI Dual Port 10/100	138603-B21
	NC3135 Fast Ethernet Module Dual 10/100 Upgrade Module for NC3134	138604-B21
	NC6132 1000 SX Upgrade Module for NC3134	338456-B23
	NC6136 Gigabit Server Adapter, 64-bit/66MHz, PCI, 1000 SX	203539-B21
	NC6170 Dual Port PCI-X 1000SX Gigabit Server Adapter	313879-B21
	NC6770 PCI-X Gigabit Server Adapter, 1000-SX	244949-B21
	NC7170 Dual Port PCI-X 1000T Gigabit Server Adapter	313881-B21
	NC7132 Gigabit Upgrade Module 10/100/1000-T	153543-B21
	NC7770 PCI-X Gigabit server adapter	244948-B21
	56K v.90 PCI Modem	239137-001
	NOTE: Any NC31XX, NC61XX, NC71XX or NC77XX NIC can be used for redundancy with the embedded NC7760 Network Controller	
Management Options	Remote Insight Lights-Out Edition II	227251-001
Security	HP/Atalla AXL600L SSL Accelerator Card for ProLiant Servers	524545-B21
Monitors	*Essential Series*	
	Compaq S9500 CRT Monitor (19-inch, Carbon/Silver)	261615-003
	Compaq S7500 CRT Monitor (17-inch, Carbon/Silver)	261606-001
	Compaq S5500 CRT Monitor (15-inch Carbon/Silver)	261602-001
	Compaq TFT1501 Flat Panel Monitor (15-inch, Carbon/Silver)	301042-003
	Compaq TFT1701 Flat Panel Monitor (17-inch, Carbon/Silver)	292847-003
	Advantage Series	
	Compaq V7550 CRT Color Monitor (17-inch, Carbon/Silver)	261611-003
	Compaq TFT1720 Flat Panel Monitor (17-inch, Carbon/Silver)	295926-003
	Compaq FT1720M Flat Panel Monitor (17-inch, Carbon/Silver, includes speaker, USB port, headphone)	301958-003
	Compaq TFT1520 Flat Panel Monitor (15-inch, Carbon/Silver)	295925-003
	Compaq TFT1520M Flat Panel Monitor (15-inch, Carbon/Silver includes speaker, USB port, headphone)	301957-003
	Performance Series	
	HP P930 CRT Monitor (19-inch, Flat-screen, Carbon/Silver)	302268-003
	HP P1130 CRT Monitor (21-inch, Flat-screen, Carbon/Silver)	302270-003
	HP L1825 Flat Panel Monitor (18-inch, Carbon/Silver)	303486-003
	HP L2025 Flat Panel Monitor (20-inch, Carbon/Silver)	303102-003
	Compaq TFT1825 Flat Panel Monitor (18-inch, Carbon/Silver)	296751-003
	Compaq TFT2025 Flat Panel Monitor (20-inch, Carbon/Silver)	285550-003
	Rackmount Flat Panel Monitors	
	TFT5110R Flat Panel Monitor (Carbon)	281683-B21
	NOTE: Monitors larger than 17" may be too heavy for use in rack systems	

Tape Drives

NOTE: In order to install certain tape drives internally, you may need to remove the rails that come standard on the drives and then re-insert the screws in the mounting holes. To ensure proper fit, install the mounting screws as described in the tape option kit.

Internal and External DAT Tape Drives

Internal 12/24-GB DAT Drive (Opal)	295513-B22

NOTE: Please see the 12/24-GB DAT Drive QuickSpecs for additional options such as cassettes and for an up-to-date listing of the latest O/S Support details, please see the following.
http //www5.compaq.com/products/quickspecs 10239 na/10239 na HTML

HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, Internal (Carbon)	157769-B22
HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, External (Carbon)	157770-002
HP StorageWorks Internal 20/40-GB DAT, Hot Plug (Carbon)	215488-B21

NOTE: Please see the 20/40-GB DAT Tape Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following.
http //www5.compaq.com/products/quickspecs/10426 na/10426 na HTML

Internal and External DAT 72 Tape Backup Drive

HP StorageWorks DAT 72 Tape Drive Internal (Carbon)	Q1525A
HP StorageWorks DAT 72 Tape Drive, External (Carbon)	Q1527A
HP StorageWorks DAT 72h Internal Hot Plug (Carbon)	Q1529A

NOTE: Please see the DAT 72 Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11597 na/11597_na.HTML

Internal and External LTO Ultrium Tape Drives

HP StorageWorks Ultrium 215 Tape Drive for ProLiant, Internal (Carbon)	Q1543A
HP StorageWorks Ultrium 215 Tape Drive for ProLiant, External (Carbon)	Q1544A

NOTE: Please see the HP StorageWorks Ultrium 230 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://h18006 www1 hp.com/products/quickspecs/11678 na/11678 na html

HP StorageWorks LTO Ultrium 230 Tape Drive, Internal (Carbon)	Q1515A
HP StorageWorks LTO Ultrium 230 Tape Drive, External (Carbon)	Q1516A

NOTE: Please see the HP StorageWorks LTO Ultrium QuickSpecs for additional options such as data and cleaning cartridges, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11415 na/11415 na HTML

HP StorageWorks Ultrium 460 tape drive for ProLiant, Internal (Carbon)	Q1518A
HP·StorageWorks Ultrium 460 tape drive for ProLiant, External (Carbon)	Q1519A

NOTE: Please see the HP StorageWorks Ultrium 460 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for an up-to-date listing of the latest O/S Support details, please see the following
http / www5 compaq com/products quickspecs 11530 na/11530 na.HTML

Options

Internal and External AIT Tape Drives

NOTE: The Internal AIT Hot Plug Drives are supported in hot plug drive bays only. When installing a non hot plug AIT tape drive into an ML350 ProLiant server use the special screw included with the drive kit proper fit in the removable media bay.

HP StorageWorks Internal AIT 35-GB, LVD Tape Drive (Carbon)	216884-B21
HP StorageWorks External AIT 35-GB, LVD Tape Drive (Carbon)	216885-001
HP StorageWorks Internal AIT 35-GB, LVD, Hot Plug (Carbon)	216886-B21

NOTE: Please see the AIT 35-GB, LVD Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following
http://www5.compaq.com/products/quickspecs/10712_na/10712_na.HTML

HP StorageWorks AIT 50-GB Tape Drive, Internal (Carbon)	157766-B22
HP StorageWorks AIT 50-GB Tape Drive, External (Carbon)	157767-002
HP StorageWorks Internal AIT 50-GB, Hot Plug (carbon)	215487-B21
HP StorageWorks Rackmount AIT 50-GB, 3U (Single Drive)	274333-B21

NOTE: Please see the AIT 50-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10425_na/10425_na.HTML

HP StorageWorks Internal AIT 100-GB Tape Drive (Carbon)	249189-B21
HP StorageWorks External AIT 100-GB Tape Drive (Carbon)	249160-001
HP StorageWorks Internal AIT 100-GB, Hot-Plug (Carbon)	249161-B21

NOTE: Please see the AIT 100-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11062_na/11062_na.HTML

Internal and External DLT/SDLT Tape Drives

NOTE: When installing a DLT or SDLT tape drive into a ProLiant ML350, use the special screw included with the drive kit to ensure proper fit in the removable media bay.

HP StorageWorks 40/80-GB DLT Tape Drive, Internal (Carbon)	146196-B22
HP StorageWorks 40/80-GB DLT Tape Drive, External (Carbon)	146197-B23
HP StorageWorks Rackmount DLT 40/80, 3U (Single Drive)	274332-B21
HP StorageWorks Rackmount DLT 40/80, Dual-Drive, 3U (Two Drives)	274335-B21
HP StorageWorks Rackmount DLT 40/80, Tape Array III, 5U (Four Drives)	274337-B21

NOTE: Please see the 40/80-GB DLT Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10658_na/10658_na.HTML

HP StorageWorks DLT VS 40/80 Tape Drive, Internal (Carbon)	280129-B21
HP StorageWorks DLT VS 40/80 Tape Drive, External (Carbon)	280129-B22

NOTE: Please see the 40/80-GB DLT VS Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11403_na/11403_na.HTML

HP StorageWorks SDLT 110/220, Internal (carbon)	192106-B25
HP StorageWorks SDLT 110/220, External (Carbon)	192103-002
HP StorageWorks Rackmount SDLT 110/220, 3U (Single Drive)	274331-B21
HP StorageWorks Rackmount SDLT 110/220, Dual-Drive, 3U (Two Drives)	274334-B21
HP StorageWorks Rackmount SDLT 110/220, Tape Array III, 5U (Four Drives)	274336-B21

NOTE: Please see the SDLT 110/220-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10772_na/10772_na.HTML

HP StorageWorks SDLT 160/320, Internal (carbon)	257319-B21
HP StorageWorks SDLT 160/320, External (carbon)	257319-001

NOTE: Please see the SDLT 160/320GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11406_na/11406_na.HTML

Internal and External DAT Autoloader

20/40-GB DAT 8 Cassette Autoloader Internal (Opal)	166504-B21
20/40-GB DAT 8 Cassette Autoloader External (Opal)	166505-001

NOTE: Please see the 20/40-GB DAT DDS-4 8 Cassette Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10518_na/10518_na.HTML

Options

AIT Autoloader

HP StorageWorks AIT 35GB Autoloader, Rackmount (carbon) 280349-001

HP StorageWorks AIT 35GB Autoloader Tabletop (carbon) 292355-001

NOTE: Please see the HP StorageWorks AIT 35GB Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following.
http://www5.compaq.com/products/quickspecs/11404_na/11404_na.HTML

HP StorageWorks 1/8 Autoloader

HP StorageWorks 1/8 Autoloader, Tabletop, Ultrium 230 C9572CB

HP StorageWorks 1/8 Autoloader, Tabletop, DLT VS80 C9264CB

HP StorageWorks 1/8 Autoloader, Rackmount kit C9266R

NOTE: Please see the HP StorageWorks 1/8 Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following
http://www5.compaq.com/products/quickspecs/11496_na/11496_na.HTML

SSL1016 tape autoloader

SSL1016 DLT1 tape autoloader (includes two 8-cartridge magazines and a barcode reader) 330815-B21

NOTE: Please see the SSL1016 DLT1 tape autoloader Quick Specs for additional information
http://h18000.www1.hp.com/products/quickspecs/11626_na/11626_na.HTML

SSL1016 SDLT 160/320 tape autoloader (includes two 8-cartridge magazines and a barcode reader) 330816-B21

NOTE: Please see the SSL1016 SDLT160/320 tape autoloader Quick Specs for additional information:
http://h18000.www1.hp.com/products/quickspecs/11609_na/11609_na.HTML

Add-on drives and accessories

SSL1016 DLT/SDLT 8-cartridge magazine 268664-B22

Rackmount Tape Drive Kits

3U Rackmount Kit 274338-B21

NOTE: The 3U Rackmount Kit (PN 274338-B21) can support up to (2) full-height or (4) half-height tape drives and compatible with multiple Single-Ended and LVD SCSI Tape Drives including the 12/24-GB DAT, 20/40-GB DAT, DAT 72-GB, 20/40-GB DAT DDS-4 8 Cassette Autoloader, AIT 35GB LVD, AIT 50GB, AIT 100-GB, 40/80-GB DLT, DLT VS 40/80-GB, SDLT 110/220-GB, SDLT 160/320-GB, Ultrium 215, Ultrium 230 and Ultrium 460 Tape Drives

5U Rackmount Kit 274339-B21

NOTE: The 5U Rackmount Kit (PN 274339-B21) can support up to (4) full-height tape drives and is compatible with DLT/SDLT/LTO tape drives including the 40/80-GB DLT, SDLT 110/220, SDLT 160/320, Ultrium 230, and Ultrium 460 Tape Drives.

NOTE: Please see the Rackmount Tape Drive Kits QuickSpecs for additional information regarding these kits, please see the following.
http://www5.compaq.com/products/quickspecs/10854_na/10854_na.HTML

Tape Storage Enclosure Cable Kits

LVD Cable Kit, VHDCI/HD68 168048-B21

NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Array III only.

LVD Cable Kit, HD68/HD68 242381-B21

NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Array III only

Tape Automation

StorageWorks SSL2000 small system library

SSL2020 – AIT50 based library with up to 2 drives and 20 slots

SSL2020 AIT Mini-Library 1 drive, 20 slot Table Top	175195-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Table Top	175195-B22
SSL2020 AIT Mini-Library 1 drive, 20 slot Rackmount	175196-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Rackmount	175196-B22
SSL2020 AIT Library Pass Thru with Transport	175312-B21

Add-on drives and accessories

SSL2020 AIT Library Pass Thru Extender	175312-B22
AIT 50GB Drive Add-On LVD Drive for SSL2020 AIT Library	175197-B21
19 Slot Magazine for SSL2020 AIT Library	175198-B21
AIT 50-GB Data Cassette (5 pack)	152841-001
AIT Cleaning Cassette	402374-B21

NOTE: Please see the SSL2020 Automated AIT Tape Library Solution QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10580_na/10580_na.HTML

StorageWorks MSL6000 and MSL5000 Departmental tape libraries

MSL6060L1 – Ultrium 460 1 based departmental library up to 4 drives and 60 slots

MSL6060L1, 0 DRV Ultrium 460 RM Library	331196-B23
MSL6060L1, 2 DRV Ultrium 460 RM Library	331195-B21
MSL6060L1, 2 DRV Ultrium 460 TT Library	331196-B21
MSL6060L1FC, 2 DRV Ultrium 460 embedded Fibre RM Library	331196-B22

NOTE: Please see the StorageWorks MSL6060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11608_na/11608_na.HTML

StorageWorks MSL6000 and MSL5000 departmental libraries

MSL5060L1 – LTO Ultrium 1 based departmental library up to 4 drives and 60 slots

MSL5060L1, 0 DRV LTO1 RM Library	301899-B21
MSL5060L1, 2 DRV LTO1 RM Library	301899-B22
MSL5060L1, 2 DRV LTO1 TT Library	301900-B21
MSL5060L1FC, 2 DRV LTO1 RM-with integrated FC router	301899-B23

NOTE: Please see the StorageWorks MSL5060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at.
http://www5.compaq.com/products/quickspecs/11438_na/11438_na.HTML

MSL5052S2 – SDLT160 based departmental library up to 4 drives and 52 slots

MSL5052S2, RM 0 DRV SDLT ALL	255102-B21
MSL5052S2, 2 DRV SDLT2 TT LIB	293476-B21
MSL5052S2, 2 DRV SDLT2 RM LIB	293474-B21
MSL5052S2FC 2 DRV SDLT2 RM- with integrated FC router	293474-B24

NOTE: Please see the StorageWorks MSL5052S2 Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at
http://www5.compaq.com/products/quickspecs/11412_na/11412_na.HTML

Options

MSL6030 – LTO Ultrium 460 mid-range library up to 2 drives and 30 slots

MSL6030 0-drive, LTO, LVDS, RM	330731-B21
MSL6030 1-drive, LTO Gen2, LVDS, RM	330731-B22
MSL6030 2-drive, LTO Gen2, LVDS, RM	330731-B23
MSL6030 1-drive, LTO Gen2, Fibre, RM	330731-B24
MSL6030 2-drive, LTO Gen2, Fibre, RM	330731-B25
MSL6030 1-drive, LTO Gen2, LVDS, TT	330788-B21
MSL6030 2-drive, LTO Gen2, LVDS, TT	330788-B22

MSL5030L1 – LTO Ultrium 1 mid-range library up to 2 drives and 30 slots

MSL5030L1, 0 DRV LTO1 RM Library	301897-B21
MSL5030L1, 1 DRV LTO1 RM Library	301897-B22
MSL5030L1, 2 DRV LTO1 RM Library	301897-B23
MSL5030L1, 1 DRV LTO1 TT Library	301898-B21
MSL5030L1, 2 DRV LTO1 TT Library	301898-B22
MSL5030L1FC, 1 DRV LTO1 RM- with integrated FC router	301897-B24

NOTE: Please see the StorageWorks MSL5030 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11439_na/11439_na.HTML

MSL5026S2 – SDLT160 based mid-range library up to 2 drives and 26 slots	
MSL5026S2, 0 DRV SDLT2 RM Library	293472-B21
MSL5026S2, 1 DRV SDLT2 RM Library	293472-B22
MSL5026S2, 2 DRV SDLT2 RM Library	293472-B23
MSL5026S2, 1 DRV SDLT2 TT Library	293473-B21
MSL5026S2, 2 DRV SDLT2 TT Library	293473-B22
MSL5026S2FC, 1 DRV SDLT2 RM- with integrated FC router	293472-B24
MSL5026S2FC, 2 DRV SDLT2 RM- with integrated FC router	293472-B25

NOTE: Please see the StorageWorks MSL5026SL Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11453_na/11453_na.HTML

MSL5026SL Graphite – SDLT110 based mid-range library up to 2 drives and 26 slots	
MSL5026SL, 1 DRV SDLT TT, graphite	302511-B21
MSL5026SL, 2 DRV SDLT TT, graphite	302511-B22
MSL5026SL, 1 DRV SDLT RM, graphite	302512-B21
MSL5026SL, 2 DRV SDLT RM, graphite	302512-B22

NOTE: Please see the StorageWorks MSL5026SL Graphite Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11440_na/11440_na.HTML

MSL5026DLX– 40/80GB DLT based mid-range library up to 2 drives and 26 slots	
MSL5026DLX, 1 40/80GB DLT, LVD, TT	231821-B21
MSL5026DLX, 2 40/80GB DLT, LVD, TT	231821-B22
MSL5026DLX, 1 40/80GB DLT, LVD, RM	231891-B21
MSL5026DLX, 2 40/80GB DLT, LVD, RM	231891-B22

NOTE: Please see the StorageWorks MSL5026DLX Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10860_na/10860_na.HTML

MSL6000 and MSL5000 Add-on drives & accessories	
MSL SDLT 160/320 Upgrade DRV	293475-B21
MSL Ultrium 460 upgrade drive in hot plug canister	330729-B21
MSL5000 SDLT 110/220 Upgrade DRV	231823-B22
MSL5000 40/80GB DLT Upgrade DRV	231823-B21
MSL Dual Magazine DLT (2 X 13 slot magazines)	232136-B21
MSL Universal passthrough mechanism	304825-B21
MSL 5U passthrough extender	231824-B22
MSL 10U passthrough extender	231824-B23
MSL Dual Magazine - Ultrium	301902-B21

Options

Smart Array Cluster Storage	Smart Array Cluster Storage	201724-B21
	Smart Array Cluster Storage Redundant Controller Option Kit	218252-B21
	128MB Cache Module for Smart Array 5302 Controller	153506-B21
	256MB Battery Backed Cache Module	254786-B21
	4-Port Shared Storage Module with Smart Array Multipath Software for Smart Array Cluster Storage	292944-B21

NOTE: All 128MB Cache modules must be removed when 256MB cache modules are installed.
NOTE: Please see the Smart Array Cluster Storage QuickSpecs for additional information including configuration steps and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11050_na/11050_na.html

External Storage – Tower and Rack	StorageWorks Enclosure Model 4314T (tower)	190210-001
	StorageWorks Enclosure Model 4314R (rack-mountable)	190209-001
	StorageWorks Enclosure Model 4354R (rack-mountable)	190211-001

NOTE: The StorageWorks Enclosure 4300 Family support the Wide Ultra2/Ultra3 1" Hot Plug Hard Drives.

	Redundant Power Supply Option	119826-B21
	Ultra3 Single Bus I/O Module Option	190212-B21
	Ultra3 Duol Bus I/O Module Option	190213-B21
	StorageWorks Enclosure Tower to Rack Conversion Kit	150213-B21

MSA1000	MSA1000	201723-B22
	MSA1000 Controller	218231-B22
	MSA Fibre Channel I/O Module	218960-B21
	MSA1000 Fabric Switch	218232-B21
	MSA1000 Fibre Channel Adapter (FCA) 2101	245299-B21
	HP StorageWorks msa hub 2/3	286763-B21

NOTE: Please see the StorageWorks by Compaq Modular SAN Array 1000 QuickSpecs for additional options and configuration information at:
http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML

Network Storage Router	M2402 2FCX 4SCSI LVD Network Storage Router	262653-B21
	M2402 2FCX 4SCSI HVD Network Storage Router	262654-B21
	M2402 4 channel LVD SCSI Module	262655-B21
	M2402 4 channel HVD SCSI Module	262660-B21
	M2402 2 channel FC Module	262661-B21
	MSL5000 Embedded Router Fibre Option Kit - Graphite	262672-B21
	MSL5026 Embedded Router Fibre Option Kit - Opal	286694-B21

StorageWorks Options	StorageWorks Fibre Channel SAN Switches 8-EL	176219-B21
	StorageWorks SAN Switch 2/8-EL	258707-B21
	StorageWorks SAN Switch 2/16-EL	283056-B21
	StorageWorks SAN Switch 2/8-EL Upgrade Kit	288162-B21
	StorageWorks SAN Switch 2/16-EL Upgrade Kit	288250-B21

Options

UPS and PDU Power Cord Matrix	Please see the UPS and PDU cable matrix that lists cable descriptions, requirements, and specifications for UPS and PDU units: ftp://ftp.compaq.com/pub/products/servers/ProLiantstorage/power-protection/powercordmatrix.pdf. NOTE: This Web site is available in English only.	
Uninterruptible Power Systems – Tower UPSs	HP UPS Model T700 (700VA, 500 Watt), Low Voltage	204015-001
	HP UPS T1000 XR (1000 VA, 700 Watts), Low Voltage	204155-001
	HP UPS T1500 XR (1440 VA, 1050 Watts)	204155-002
	HP UPS T2200 XR (1920 VA, 1600 Watts) Low Voltage	204451-001
	HP UPS T2200 XR (2200 VA, 1600 Watts) High Voltage	204451-002
Uninterruptible Power Systems – HP Rack UPSs	HP UPS R1500 XR (100 to 127)	204404-001
	HP UPS R3000 XR (120V)	192186-001
	HP UPS R3000 XR (208V)	192186-002
	Rack-Mountable UPS R6000 (208V) NOTE: UPS R6000 has a hardwired input; and the UPS R12000 XR has a hardwired input and output connection.	347207-001
	HP UPS R12000 XR N+ x (200-240V) NOTE: The UPS R12000 XR has a hardwired input and output. NOTE: HP UPS R6000 has a hardwired input; the UPS R12000 XR has a hardwired input and output connection.	207552-B22
UPS Options	SNMP Serial Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 3000VA	192189-B21
	Six Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 3000VA.	192185-B21
	High to Low Voltage Transformer (250VA) NOTE: Supports R6000 UPS series only. 2.5A @ 125 Volts max output across two NEMA 5-15.	388643-B21
	Extended Runtime Module, T1000 XR	218967-B21
	Extended Runtime Module, T1500 XR/T2200 XR	218969-B21
	Extended Runtime Module, R1500 XR NOTE: 2U each, two ERM maximum.	218971-B21
	Extended Runtime Module, R3000 XR NOTE: 2U each, one ERM maximum.	192188-B21
	Extended Runtime Module, R6000 NOTE: 3U each, two ERM maximum.	347224-B21
	Extended Runtime Module, R12000 XR, 4U each, two ERMs maximum	217800-B21
	R12000 XR BackPlate Receptacle Kit, (2) L6-30R NOTE: The R12000 XR BackPlate Kit has a hardwired input.	325361-001
	R12000 XR BackPlate Receptacle Kit, (2) IEC-309R NOTE: The R12000 XR BackPlate Kit has a hardwired input.	325361-B21
	SNMP-EN Adapter NOTE. Supports R6000 UPS series only.	347225-B21
	Multi-Server UPS Card NOTE. Supports R6000 UPS series only	123508-B21
	Scalable UPS Card NOTE: Supports R6000 UPS series only	123509-B21

Options

Modular PDUs 1U/0U (Up to 32 outlets) NOTE: 1U/0U mounting brackets shipped with the unit (optimized for 10000 and 9000 series racks).	HP Modular Power Distribution Units (mPDU), Low Volt Model, 24A (100-127 VAC) NOTE: This mPDU (252663-D7) may also be used to connect the low volt model of the UPS R3000 XR.	252663-D71
	HP Modular Power Distribution Units (mPDU), High Volt Model, 24A (200-240 VAC)	252663-D72
	HP Modular Power Distribution Units (mPDU), High Volt Model, 40A (200-240 VAC) NOTE: This mPDU (252663-B21), 40A model has a hardwired input.	252663-B21
	HP Modular Power Distribution Units (mPDU), High Volt Model, 16A (200-240 VAC) NOTE: This PDU has a detachoble input power cord and allows for adaptability to country specific power requirements. This model may also be used with the high volt UPSs R3000 XR and R6000. Order cable PN 340653-001. NOTE: Please see the following Modular Power Distribution Unit (Zero-U/1U Modular PDUs) QuickSpecs for additional options including shorter jumper cables and country specific power cords http://www5.compaq.com/products/quickspecs/ 104 na/ 041 na HTML	252663-B24
PDU Options	Third Party Modular PDU Modular Kit NOTE: This kit allows you to mount the Modular PDUs in (1U configuration only) in racks other than the 9000/10000 Series racks (any racks using the standard 19' rail, including the 7000 Series racks). For more details please refer the Modular PDU QuickSpecs.	310777-B21
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (1 per pack)	142257-006
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (15 per pack)	142257-007
USB Options	USB Easy Access Keyboard (carbon)	267146-008
	USB Easy Access Keyboard (carbonite)	DC168B#ABA
	USB 2-Button Scroll Mouse (carbon)	195255-B25
	USB 2-Button Scroll Mouse (carbonite)	DC172B
	USB Floppy	304707-B21
Other	Enhanced Keyboard (Carbon)	296435-005
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (HD68)	159547-B22
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (VHDCI) NOTE: The ProLiont ML330/ML350 Internal to External SCSI Cable Option Kits (PN 159547-B21 and 333370-B21) are supported by the ML330/ML350 Family.	333370-B21
Rack Builder	Please see the Rack Builder for configuration assistance at http /www.compaq com/rackbuilder	
Rack Conversion Kit	ProLiant ML350 Generation 3 Tower to Rack Conversion Kit (CPQ branded)	290683-B21

HP Rack 10000 Series (Graphite Metallic)	HP S10614 (14U) Rack Cabinet - Shock Pallet	292302-B22
	HP 10842 (42U) Rack Cabinet - Pallet	257415-B21
	HP 10842 (42U) Rack Cabinet - Shock Pallet	257415-B22
	HP 10647 (47U) – Pallet	245160-B21
	HP 10647 (47U) – Crated	245160-B23
	HP 10642 (42U) – Pallet	245161-B21
	HP 10642 (42U) – Shock Pallet	245161-B22
	HP 10642 (42U) – Crated	245161-B23
	HP 10636 (36U) – Pallet	245162-B21
	HP 10636 (36U) – Shock Pallet	245162-B22
	HP 10636 (36U) – Crated	245162-B23
	HP 10622 (22U) – Pallet	245163-B21
	HP 10622 (22U) – Shock Pallet	245163-B22
	HP 10622 (22U) – Crated	245163-B23

NOTE: -B21 (pallet) used to ship empty racks shipped on a truck
-B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels)
-B23 (crated) used for air shipments of empty racks

NOTE: It is mandatory to use a shock pallet in order to ship racks with equipment installed. Not all Compaq equipment is qualified to be shipped in the Rack 10000 series.

NOTE: Please see the Rack 10000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color:
http://www5.compaq.com/products/quickspecs/10995_na/10995_na.HTML

NOTE: For additional information regarding Rack Cabinets, please see the following URL:
http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html
NOTE: This Web site is available in English only.

Compaq Rack 9000 Series (opal)	Compaq Rack 9142 (42U) – Pallet	120663-B21
	Compaq Rack 9142 (42U) – Shock Pallet	120663-B22
	Compaq Rack 9142 (42U) – Crated	120663-B23

NOTE: B21 (pallet) used to ship empty racks shipped on a truck
B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels)
B23 (crated) used for air shipments of empty racks

NOTE: Please see the Rack 9000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color.
http://www5.compaq.com/products/quickspecs/10366_na/10366_na.HTML

NOTE: For additional information regarding Rack Cabinets, please see the following URL:
http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.htm
NOTE: This Web site is available in English only

Options

Rack Options for HP Rack 10000 Series	Rack Blanking Panels – Graphite (Multi)	253214-B26
	NOTE: Contains one each of 1U, 2U, 4U and 8U.	
	Rack Blanking Panels – Graphite (1U)	253214-B21
	NOTE: The Rack Blanking Panel: (PN 253214-B21) contains 10 each of (1U).	
	Rack Blanking Panels – Graphite (2U)	253214-B22
	NOTE: The Rack Blanking Panels (PN 253214-B22) contains 10 each of (2U).	
	Rack Blanking Panels – Graphite (3U)	253214-B23
	NOTE: The Rack Blanking Panels (PN 253214-B23) contains 10 each of (3U).	
	Rack Blanking Panels – Graphite (4U)	253214-B24
	NOTE: The Rack Blanking Panels (PN 253214-B24) contains 10 each of (4U)	
	Rack Blanking Panels – Graphite (5U)	253214-B25
	NOTE: The Rack Blanking Panels (PN 253214-B25) contains 10 each of (5U)	
	600mm Stabilizer Kit – Graphite	246107-B21
	800mm Wide Stabilizer Kit (Graphite)	255488-B21
	NOTE: Supported by the Rack 10842 cabinet only	
	Baying Kit for Rack 10000 series (Carbon)	24892[illegible]
	42U Side Panel – Graphite Metallic	246099-B21
	110V Fan Kit (Graphite)	257413-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 5-15P.	
	220V Fan Kit (Graphite)	257414-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 6-15P.	
	36U Side Panel – Graphite Metallic	246102-B21
	47U Side Panel – Graphite Metallic	255486-B21
	9000/10000 Series Offset Baying Kit (42U)	248931-B21
	NOTE: This kit can be used to connect 9000 and 10000 series racks of the same U height together. Kit contents include hardwore for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	
	NOTE: For additional information regarding Rack Options, please see the following URL http://h18000.www [illegible] torage rack-ptions/index html	
	NOTE: This Web site is available in English only	

Options

Rack Options for Compaq Rack 9000 Series	Baying/Coupling Kit	120669-B21
	42U Side Panel NOTE: The 42U Side Panel (PN 120670-B21) supports the Compaq Rack 9142 and Compaq Rack 9842.	120670-B21
	36U Side Panel NOTE: The 36U Side Panel (PN 120671-B21) supports the Compaq Rack 9136.	120671-B21
	600mm Stabilizer Option Kit	120673-B21
	800mm Stabilizer Option Kit (Opal) NOTE: The 800mm Stabilizer Kit (PN 234493-B21) supports the Rack 9842 only.	234493-B21
	9142 Extension Kit NOTE: The 9142 Extension Kit (PN 120679-B21) supports the Compaq Rack 9142 only.	120679-B21
	Stabilizer Option Kit	120673-B21
	Rack Blanking Panel Kit for Rack 9000 series (Opal) (U.S.) NOTE: The Rack Blanking Panel Kit (PN 169940-B21) contains 4 panels one each of 1U, 2U, 4U and 8U.	169940-B21
	Rack Blanking Panels (1U) NOTE: The Rack Blanking Panels (PN 189453-B21) contains 10 each of (1U).	189453-B21
	Rack Blanking Panels (2U) NOTE: The Rack Blanking Panels (PN 189453-B22) contains 10 each of (2U).	189453-B22
	Rack Blanking Panels (3U) NOTE: The Rack Blanking Panels (PN 189453-B23) contains 10 each of (3U).	189453-B23
	Rack Blanking Panels (4U) NOTE: The Rack Blanking Panels (PN 189453-B24) contains 10 each of (4U).	189453-B24
	Rack Blanking Panels (5U) NOTE: The Rack Blanking Panels (PN 189453-B25) contains 10 each of (5U)	189453-B25
	9136 Extension Kit	218216-B21
	9142 Short Rear Door NOTE: The 9142 Short Rear Door (PN 218217-B21) supports the Compaq Rack 9142 only	218217-B21
	Split Rear Door (Opal) NOTE: The Split Rear Door (PN 254045-B21) supports the 600 mm wide, 42U 9000 series rack.	254045-B21
	9136 Short Rear Door	218218-B21
	9142 Split Rear Door	254045-B21
	9000/10000 Offset Baying Kit (42U) NOTE: This kit can be used to connect 9000 and 10000 series racks of same U height together. Kit contents include hardware for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	248931-B21
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only	
Rack Options for Compaq Rack 7000 Series	High Air Flow Rack Door Insert for the 7122 Rack	157847-B21
	High Air Flow Rack Door Insert for the 7142 Rack (single)	327281-B21
	High Air Flow Rack Door Insert for the 7142 Rack (6-pack)	327281-B22
	Compaq Networking Cable Management Kit	292407-B21
	Compaq Rack Extension Kit for 7142	154392-B21
	NOTE. For additional information regarding Rack Cabinets, please see the following URL http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.htm NOTE. This Web site is available in English only	

Options

Rack Options for Rack 7000, 9000 and 10000 Series	Monitor Utility Shelf	303606-B21
	Ballast Option Kit	120672-B21
	100kg Sliding Shelf	234672-B21
	Rack Rail Adapter Kit (25-inch depth)	120675-B21
	Cable Management D-Rings Kit	168233-B21
	Console Management Controller (CMC) Option Kit	203039-B21
	Console Management Controller (CMC) Sensors Option Kit	203039-B22
	Console Management Controller (CMC) Locking Option Kit	203039-B23
	Console Management Controller (CMC) Smoke Sensors Option Kit	203039-B24
	Server Console Switch 1 x 2 port (100 to 230 VAC)	120206-001
	Server Console Switch 1 x 4 port (100 to 230 VAC)	400336-001
	Server Console Switch 1 x 8 port (100 to 230 VAC)	400337-001
	Server Console Switch 2 x 8 port (100 to 230 VAC)	400338-001
	Server Console Switch 2 x 8 port (48 VDC)	400542-B21
	IP Console Switch Box, 1x1x16	262585-B21
	IP Console Switch Box, 3x1x16	26258[illegible]
	IP Console Interface Adapter, 8 pack	262587-B21
	IP Console Interface Adapter, 1 pack	262588-B21
	IP Console Expansion Module	262589-B21
	KVM 9 PIN Adapter (4 Pack)	149361-B21
	CPU to Server Console Cable, 12'	110936-B21
	CPU to Server Console Cable, 20'	110936-B22
	CPU to Server Console Cable, 40'	110936-B23
	CPU to Server Console Cable, 3'	110936-B24
	CPU to Server Console Cable, 7'	110936-B25
	CPU to Server Console Cable (Plenum Rated) 20'	149363-B21
	CPU to Server Console Cable (Plenum Rated) 40'	149364-B21
	IP CAT5 Cable 3', 4 pack	263474-B21
	IP CAT5 Cable 6', 8 pack	263474-B22
	IP CAT5 Cable 12', 8 pack	263474-B23
	IP CAT5 Cable 20', 4 pack	263474-B24
	IP CAT5 Cable 40', 1 pack	263474-B25
	Switch Box Connector Kit (115 V)	144007-001
	Switch Box Connector Kit (230 V)	14400[illegible]2
	1U Rack Keyboard & Drawer (Carbon)	257054-001
	NOTE: The 1U Rack Keyboard & Drawer (PN 257054-001) is to be used with the Keyboards for Racks with Trackball (PN 158649-001).	
	TFT5600 Rack Keyboard Monitor	221546-001
	Input Device Adjustable Rails	287139-B21
	NOTE Input Device Adjustable Rails 287139 B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	
	Input Device Telco Rail	287138-B21
	NOTE: Input Device Telco Rails (287138-B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks	
	Keyboard/Monitor/Mouse extension cables	169989-001
	NOTE: For additional information regarding Rack Options, please see the following URL http //h18000 www1 hp com products servers [illegible] rack options index htm	
	NOTE: This Web site is available in English only	

HP Factory Express

Factory Installation, Racking, and Customization Services

Factory Express Server Configuration Level 1	293355-888

NOTE: Free Installation of HP Options - Installation of HP Options memory, NICs, hard drives, controllers, processors, I/O cards, pre-install standard OEM OS image, and tape drives. Installation fees will apply to all non-HP certified hardware and asset tags.
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Factory Express Server Configuration Level 2	266326-888

NOTE Includes Level 1 Customer Intent of a ProLiant server and options configuration, OS installation, custom image download, IP addressing, network setting, and custom packaging. Customer unique requirements (quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, and RILOE). Customer access, validation and control through VPN (price/server).
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Factory Express Rack Integration Level 3 with 1 - 3 servers or storage enclosures	325736-888
Factory Express Rack Integration Level 3 with 4 - 9 servers or storage enclosures	232539-888
Factory Express Rack Integration Level 3 with 10 or more servers or storage enclosures	325735-888

NOTE: Includes Level 1 Customer Intent for standard mounted servers and storage units plus standard cable mgmt, RAID configuration, servers & storage, power distribution, networking gear and accessories (price/ra520ck).
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Factory Express Rack Integration Level 4 with 1 - 3 servers or storage enclosures	325734-888
Factory Express Rack Integration Level 4 with 4 - 9 servers or storage enclosures	232540-888
Factory Express Rack Integration Level 4 with 10 or more servers or storage enclosures	325733-888

NOTE: Includes Level 2 Customer Intent plus customer defined cable management and naming convention, customer furnished image download, IP addressing, cluster configurations (SQL, External storage RAID). Quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, RILOE). Customer access and validation through VPN (price/rack).
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Factory Express Rack Integration Level 5 with 1 - 3 servers or storage enclosures	325732-888
Factory Express Rack Integration Level 5 with 4 - 9 servers or storage enclosures	232541-888
Factory Express Rack Integration Level 5 with 10 or more servers or storage enclosures	325731-888

NOTE Includes Level 4 Customer Intent plus Custom SW layering and extended test, Customer access, validation and control through VPN, Clustered racks with networking gear and/or external storage array, Start-up installation services custom quote. (price/rack)
NOTE: Factory Express Engineered Solution Level 6 is a custom solutions available through Factory Express Please contact a your local reseller or Account Manager
NOTE: Available on ProLiant ML370 G3 Rack Models Only.

Service and Support Offerings (HP Care Pack Services)

Hardware Services On-site Service

4-Hour On-site Service, 5-Day x 13-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL3EC-36
4-Hour On-site Service, 5-Day x 13-Hour, 3 Years (U.S. Part Number)	331045-002
4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL7EC-36
4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	162675-002
6-Hour Call to Repair, On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-ELCEC-36
6-Hour Call to Repair, On-site Service 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	331046-002

Options

Installation & Start-up Services

Hardware Installation (Canadian Part Number)	FP-ELINS-EC
Hardware Installation (U.S. Part Number)	401791-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	240013-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (Canadian Part Number)	FM-MSTEC-01
Installation & Start-Up of a ProLiant server and Linux O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	331051-002
Installation & Start-Up of a ProLiant server and Linux O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (Canadian Part Number)	FM-LSTEC-01

Support Plus

Onsite HW support, 8am-9pm, M-F, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	239929-002
Onsite HW support, 8am-9pm, M-F, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-M01E1-36
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	331049-002
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-L01E1-36

Support Plus 24

Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number)	239930-002
Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canadian Part Number	FM-M02E1-36
Onsite HW support 24x7, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number	331050-002
Onsite HW support 24x7, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canadian Part Number	FM-L02E1-36

CarePaq Priority Services for ProLiant Servers – Priority Silver

24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Manager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (2-5-2 Part Number for Canada)	FM-M04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (2-5-2 Part Number for Canada)	FM-M24E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (2-5-2 Part Number for Canada)	FM-N04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (2-5-2 Part Number for Canada)	FM-N24E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Manager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (6-3 Part Number for U.S.)	239932-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (6-3 Part Number for U.S.)	239934-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (6-3 Part Number for U.S.)	239972-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (6-3 Part Number for U.S.)	239974-002

NOTE: For more information, customer/resellers can contact http://www.hp.com/services/carepack

Memory

HP ProLiant ML350 G3 Array Models

The ML350 G3 supports both interleaved and non-interleaved memory configurations. Array models ship standard with one 512MB DIMM, non-interleaved. For best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory and installing in pairs is not required. Add any combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory

512MB (expandable to 8GB) of 2-way interleoving capoble PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models, with Advanced ECC capabilities (1x 512MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect and correct single bit memory errors while Advanced ECC extends this coverage to include protection against multiple simultaneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within a single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standard Memory Plus Optional Memory

Up to 6.7 GB of total memory can be implemented with the installation of three optional PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory

Up to 8.2 GB of total memory can be implemented with the removal of the standard 512-MB DIMM and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

NOTE: Charts do not represent all possible memory configurations

		Slot 1	Slot 2	Slot 3	Slot 4
Standard	512 MB	512 MB	Empty	Empty	Empty
Optional	6656 MB	512 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB
2x1 Interleaved Memory (Recommended)		Pair 1		Pair 2	
	Total Memory	Slot 1	Slot 2	Slot 3	Slot 4
Recommended Configurations for Array Models	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

Following are memory options available from HP:

● 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
● 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21
● 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21

NOTE: To invoke interleaving in your array model, order this kit for a total of 1-GB of interleaved memory.

● 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
● 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21

HP ProLiant ML350 G3 Non-Array Models

The ML350 G3 supports both interleaved and non-interleaved memory configurations. Base models ship standard with one 256MB DIMM, non-interleaved. For best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory and installing in pairs is not required. Add any combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory

256MB (expandable to 8GB) of 2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advanced ECC capabilities (1x 256MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect and correct single bit memory errors while Advanced ECC extends this coverage to include protection against multiple simultaneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within a single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standord Memory Plus Optional Memory

Up to 6.4 GB optional memory is available with the installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory

'Jp to 8.2 GB of memory is available with the removal of the standard 256-MB of memory and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMM installed.

NOTE: Charts do not represent all possible memory configurations

Memory					
		Slot 1	Slot 2	Slot 3	Slot 4
Standard	256 MB	256 MB	Empty	Empty	Empty
Optional	6400 MB	256 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB
Recommended Configurations for Base Models	Total Memory Desired	1	2	3	4
	512 MB	256 MB	256 MB	Empty	Empty
	1 GB	256 MB	256 MB	256 MB	256 MB
	1.5 GB	256 MB	256 MB	512 MB	512 MB
Recommended Configurations for Array models	Total Memory Desired	1	2	3	4
	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

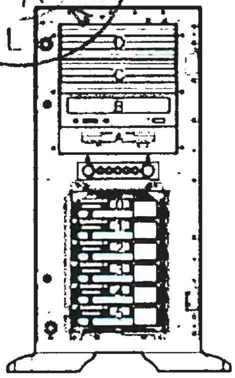
Following are memory options available from HP:

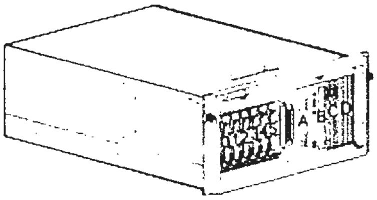
● 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
● 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21

NOTE: To invoke interleaving in your base model, order this kit for a total of 512MB of interleaved memory.

● 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21
● 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
● 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21

Storage





0 - 5	6 x 1 in SCSI Hard Drive Bays
A	3.5 in Diskette Drive
B	48x CD-ROM
C, D	Available half height bay

Drive Support

	Quantity Supported	Position Supported	Controller
Removable Media			
1.44-MB Diskette Drive	Up to 1	A	Integrated
IDE (ATAPI) CD-ROM Drive	Up to 2	B, C, D	Integrated IDE (ATAPI)
DVD-ROM Drive Option Kit	Up to 2	B, C, D	Integrated IDE
ML3xx Two Bay Hot Plug SCSI Drive Cage	Up to 1	C, D	Integrated SCSI

Storage

Hard Drives

Ultra320 Hot Pluggable Drives

	Quantity Supported	Position Supported	Controller
1-inch 146.8-GB 10,000 rpm 72.8-GB 10,000 rpm 36.4-GB 10,000 rpm 72.8-GB 15,000 rpm 36.4-GB 15,000 rpm 18.2-GB 15,000 rpm	Up to 6	0-5	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standord with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

NOTE: All U320 Universal Hard Drives are backward compatible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates.

Wide Ultra320 SCSI – Non-Hot Plug

	Quantity Supported	Position Supported	Controller
1-inch 36-GB 10,000 rpm	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

External Storage

	Quantity Supported	Position Supported	Controller
StorageWorks Enclosure 4300 Family (supports Ultra3/Ultra320 1" drives)	Up to 24	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
3U Rackmount Kit 5U Rackmount Kit	Up to 3	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
MSA 1000	Please see the MSA 1000 QuickSpecs below to determine configuration requirements	External	Please see the MSA 1000 QuickSpecs (URL below) for the latest list of supported HBAs

MSA 1000: http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTM

Storage

Maximum Storage Capacity – (StorageWorks Enclosure)

Internal	1.174 TB (6 x 146.8-GB 1" Ultra320 hot plug hard drives with standard internal drive cage + 2 x 72.8-GB 12"Ultra320 Hot plug hard drive using the optional ML3xx Two Bay Hot Plug SCSI Drive Cage)
External	49.324 TB (14 x 146.8 GB) x 24
Total	50.498 TB

Tape Drives

NOTE: For on up-to-date listing of the latest O/S Support details for each of the Tape Drives listed below, please see the following: http://www5.compaq.com/products/quickspecs/North_America/10233.htm.

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Storage Systems listed below, please see the following: http://www5.compaq.com/products/quickspecs/North_America/10809.htm.

	Quantity Supported	Position Supported	Controller
Internal AIT 100-GB, Hot Plug Internal AIT 50-GB, Hot Plug Internal AIT 35-GB, LVD Hot Plug Internal 20/40-GB DAT Drive, Hot Plug Internal DAT 72, Hot Plug *Installation of AIT/DAT hot plug drives in D + C requires the optional Two Bay Hot Plug SCSI Drive Cage (PN 244059-B21)	Up to 3	0+ 1, 2+ 3, D+ C*	Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter *NOTE: The Smart Array 532 Controller does not support the AIT 100-GB Hot Plug Tape Drive.
20/40-GB DAT DDS-4 Tape Drive Internal 12/24-GB DAT Drive Internal DAT 72	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 35GB, Autoloader	Up to 4	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT Enhanced	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT VS	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB Internal AIT 50-GB Internal AIT 35-GB, LVD Internal	Up to 2	C, D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 230, Internal LTO Ultrium 460, Internal	Up to 1	C + D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SDLT 110/220-GB, Internal SDLT 160/320-GB, Internal	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External DAT 72	2	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB External AIT 50-GB External AIT 35-GB, LVD External	2	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External 40/80-GB DLT Enhanced External 40/80-GB DLT VS External 20/40-GB DLT	Up to 3	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 215, External LTO Ultrium 230, External LTO Ultrium 460, External	Up to 2	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

Storage

SDLT 110/220-GB, External SDLT 160/320-GB, External	Up to 2	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
20/40-GB DAT 8 Cassette Autoloader External	Up to 1	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SSL2020 AIT Library	2 drives per SCSI channel	External	SAN Access Module for Smart Array 5302 Controller
MSL5026DLX (40/80GB DLT-based) MSL5026SL (SDLT-based) Library MSL5052SL (SDLT-based) Library MSL5030L (LTO-based) Library MSL5060S (LTO-based) Library	2 drives per SCSI channel	External	64-Bit/66-MHz Dual Channel Wide-Ultra3 SCSI Adapter, Alternate OS

Power Specifications

Part Number	264166-001
Spare Kit	292237-001
Operational Input Voltage Range (V rms)	90 to 264
Frequency Range (Nominal) (Hz)	47 to 63 (50/60)

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Max Rated Output Wattage Rating	500	500	500	500	500	500
Nominal Input Current (A rms)	7.8	6.7	3.7	3.4	3.2	3.0
Max Rated Input Wattage Rating (Watts)	769	758	746	735	725	714
Max. Rated VA (Volt-Amp)	785	773	761	750	739	729
Efficiency (%)	65	66	67	68	68	70
Power Factor	0.98	0.98	0.98	0.98	0.98	0.98
Leakage Current (mA)	0.31	0.36	0.65	0.69	0.72	0.75
Maximum Inrush Current (A peak)	21	24	43	46	48	50
Maximum Inrush Current duration (miliseconds)	20	20	20	20	20	20

System Specifications

ML350 Generation 3 (G3) Fully Configured

Up to 2 Processors, 4 Memory Slots, 8 Hard Drives, 5 PCI Slots, and 2 Hot Plug Power Supplies

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Fully Loaded System Input Wattage (W)	557	549	541	534	526	519
Fully Loaded System Input Current (A rms)	5.7	4.9	2.7	2.5	2.3	2.2
Fully Loaded System Thermal (BTU-Hr)	1900	1872	1846	1820	1794	1770
Fully Loaded System VA (Volt-Amp)	569	560	552	545	537	530
System Leakage with all power supplies loaded (mA)	0.63	0.72	1.30	1.38	1.44	1.50
System Inrush Current with all power supplies loaded (A)	·42	48	86	92	96	100
Power cord requirements	Nema 5-15P to IEC320-C13			Option no./Spare no: See Power Cord chart		
	IEC320-C13 to IEC320-C14			Option no./Spare no: 142257-001/142258-B21		

NOTES:

ActiveAnswers Power Calculation

Power calculator is LIVE on ActiveAnswers Web site. This is an external link

Follow this link: http://h30099.www3 hp.com configurator/powercalcs asp

NOTE: This Web site is available in English only.

To drill down to calculators:

- Click on: "ProLiant Servers"
- Click on the Server of interest. Example: ML350 G3
- Click on: "Power Calculator" link. (You moy need to scroll down to see it)

TechSpecs

System Unit – Tower	Dimensions (HxWxD) (with feet/bezel)	18.5 x 10.25 x 26 in (46.99 x 26.04 x 66.04 cm)	
	Dimensions (HxWxD) (without feet/bezel)	17.5 x 8.5 x 24 in (44.50 x 21.59 x 60.96 cm)	
	Weight(approximate)	60 lb (27.24 kg) (without hard drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110-VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors (Support for either two internal, two external, or a mix of internal/external is available. This is achieved using an internal to external SCSI cable option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	500W
	Temperature Range	Operating	50° to 95° F (10° to 35° C) (No direct sustaining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

TechSpecs

System Unit – Rack	Dimensions (HxWxD)	8.61 x19 x 24 in (21.87 x48.26 x 60.96 cm)	
	Weight(approximate)	60 lb (27.24 kg) (without hord drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110 VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors (Support for either two internal, two external, or a mix of internal/external is available. This is achieved using an internal to external SCSI cable option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	500W
	Temperature Range	Operating	50° to 95° F (10° to 35° C) (No direct sustaining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

1.44-MB Diskette Drive	LED Indicators (front panel)	Green	
	Read/Write Capacity per Diskette (high/low density)	1.44 MB/720 KB	
	Drive Supported	One	
	Drive Height	One-third	
	Drive Rotation	300 rpm	
	Transfer Rate (high/low)	500 K/250 K bits/s	
	Bytes/Sector	512	
	Sectors/Track (high/low)	18/9	
	Tracks/Side (high/low)	80/80	
	Access Times	Track-to-Track (high/low)	3/6 ms
		Average (high/low)	169/94 ms
		Settling Time	15 ms
		Latency Average	100 ms
	Cylinders (high/low)	80/80	
	Read/Write Heads	Two	

48X Max IDE (ATAPI) CD-ROM Drive	Disk	Applicable Disk	CD-ROM, CD-XA, CD-DA (Mode 1, Mode 2, Form 1 and 2)
			Photo CD (Single and Multi-session)
			Mixed Mode (Audio and Data combined)
			CD-R
		Capacity	540 MB (Mode 1, 12 cm)
			650 MB (Mode 2, 12 cm)
	Block Size	Mode 1	2,048 bytes
		Mode 2	2,340 bytes, 2,336 bytes
		CD-DA	2,352 bytes
		CD-XA	2,328 bytes
	Interface	IDE (ATAPI)	
	Access Times (typical)	Random	<100 ms
		Full-Stroke	<150 ms
	Data Transfer Rate	Sustained	3000 to 7200 KB/s (20X to 48X)
		Burst	150 KBps to 7,200 KBps
		Bus Rate	16.7 MBps
	Cache Buffer	128 KB	
	Start-up Time (typical)	< 7seconds	
	Stop Time	< 4seconds	
	Laser Parameters	Type	Semiconductor Laser GaA1As
		Wave Length	780 ± 25 nm
	Operating Conditions	Temperature	41° to 113° F (5° to 45° C)
		Humidity	10% to 80%
	Dimensions	(HxWxD, maximum)	1.7 x 5.85 x 8.11 in (4.29 x 14.86 x 20.60 cm)
		Weight	2.09 lb (0.95 kg)

NC7760 PCI Gigabit Server Adapter (embedded)	Network Interface	10Base-T/100Base-TX/1000Base-TX	
	Compatibility	IEEE 802.3 10Base-T	
		IEEE 802.3ab 1000Base-T	
		IEEE 80.3u 100Base-TX	
	Data Transfer Method	32-bit bus-master PCI	
	Network Transfer Rate	10Base-T(Half-Duplex)	10 Mb/s
		10Base-T(Full-Duplex)	20 Mb/s
		100Base-TX(Half-Duplex)	100 Mb/s
		100Base-TX(Full-Duplex)	200 Mb/s
		1000Base-TX	1000Mb/s
	Connector	RJ-45	
	Cable Support	10Base-T	Categories 3, 4 or 5 UTP; up to 328 ft (100 m)
		10/100/1000Base-TX	Category 5 UTP; up to 328 ft (100 m)

TechSpecs

Integrated Dual Channel Wide Ultra3 SCSI Adapter	Drives Supported	Up to 28 SCSI devices (14 per channel)
	Data Transfer Method	64-bit PCI bus-master
	SCSI Channel Transfer Rate	80 MB/s per channel
	Maximum Transfer Rate per PCI Bus (peak)	133 MB/s per channel
	SCSI Protocols	Wide Ultra2 SCSI Wide-Ultra SCSI-3 Fast SCSI-2
	Electrical Protocol	Low Voltage Differential (LVD)
	SCSI Termination	Active Termination
	External SCSI Connectors	Two 80-Pin VHDCI connectors
	Internal SCSI Connectors	Two 68-Pin Wide-Ultra SCSI-3 connectors

Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with the 2.8 GHz Array Models only)	Protocol	Ultra320 SCSI
	SCSI Electrical Interface	Low Voltage Differential (LVD)
	Drives Supported	Up to 6 Ultra 320, Ultra3 and Ultra2 SCSI hard drives
	SCSI Port Connectors SA-641	one internal SCSI port
	Data Transfer Method	64-Bit PCI bus-master
	PCI Bus Speed	64-bit, 133-MHz PCI-X (1 GB/s maximum bandwidth)
	PCI	3.3 volt PCI slot compatibility only
	Simultaneous Drive Transfer Channels	Two
	Channel Transfer Rate	320-MB/s total; 320-MB/s per channel
	Software upgradeable Firmware	Yes
	Cache Memory	64-MB DRAM used for code, transfer buffers, and non-battery backed read cache
	Logical Drives Supported	32
	Maximum Capacity	880.8 GB (6 X 146.8 GB)
	Memory Addressing	64-bit, supporting servers memory greater than 4 GB
	RAID Support	RAID 5 (Distributed Data Guarding) RAID 1+ 0 (Striping & Mirroring) RAID 1 (Mirroring) RAID 0 (Striping)
	Upgradeable Firmware	2-MB Flashable ROM
	Disk Drive and Enclosure Protocol Support	Ultra 320, Ultra2 and Ultra3
	Warranty	Maximum: The remaining warranty of the HP server product in which it is installed (to a maximum three-year limited warranty) Minimum: One-year, on-site limited warranty Pre-Failure Warranty: Drives attached to the Smart Array Controller and monitored under Insight Manager are supported by a Pre-Failure (replacement) Warranty. For complete details, consult the HP Support Center or refer to your HP Server Documentation.

Video Controller	Controller Chip	ATI RAGE XL
	Video DRAM	8 MB Video SDRAM
	Data Transfer Method	32-bit PCI
	Support Resolution	Supported Color Depths:
	640 x 480	16.7M, 64K, 256, 16
	800 x 600	16.7M, 64K, 256, 16
	1024 x 768	16.7M, 64K, 256, 16
	1152 x 864	16.7M, 64K, 256, 16
	1280 x 1024	16.7M, 64K, 256, 16
	1600 x 1200	64K, 256, 16
	Connector	VGA

The information contained herein is subject to change without notice.

Microsoft and Windows NT are US registered trademarks of Microsoft Corporation. Intel is a US registered trademark of Intel Corporation.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Apêndice FD

CHAPTER 34

Configuring Local SPAN and RSPAN

This chapter describes how to configure local Switched Port Analyzer (SPAN) and remote SPAN (RSPAN) on the Catalyst 6500 series switches. The Catalyst 6500 series switches support RSPAN with Release 12.1(13)E and later releases.

This chapter consists of these sections:

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

Understanding How Local SPAN and RSPAN Work

These sections describe how local SPAN and RSPAN work:

Local SPAN and RSPAN Overview

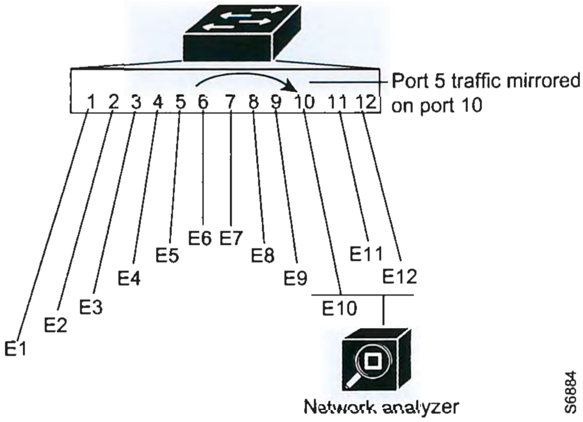
Local SPAN and RSPAN both select network traffic to send to a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. SPAN does not affect the switching of network traffic on source ports or VLANs. SPAN sends a copy of the packets received or transmitted by the source ports and VLANs to the destination port. You must dedicate the destination port for SPAN use.

These sections provide an overview of local SPAN and RSPAN:

Local SPAN Overview

Local SPAN supports source ports, source VLANs, and destination ports on the same Catalyst 6500 series switch. Local SPAN copies traffic from one or more source ports in any VLAN or from one or more VLANs to a destination port for analysis (see Figure 34-1). For example, as shown in Figure 34-1, all traffic on Ethernet port 5 (the source port) is copied to Ethernet port 10. A network analyzer on Ethernet port 10 receives all network traffic from Ethernet port 5 without being physically attached to Ethernet port 5.

Figure 34-1 Example SPAN Configuration



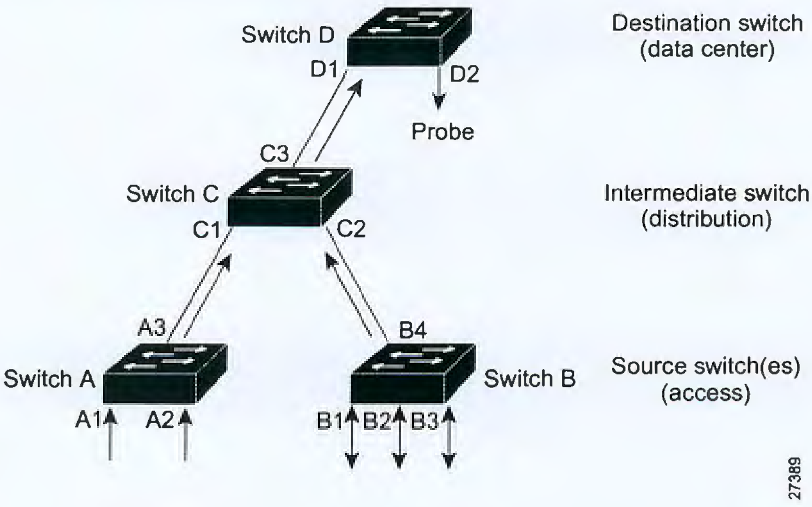
RSPAN Overview

RSPAN supports source ports, source VLANs, and destination ports on different switches, which provides remote monitoring of multiple switches across your network (see Figure 34-2). The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches.

The RSPAN source ports can be trunks carrying the RSPAN VLAN. Local SPAN and RSPAN do not monitor the RSPAN traffic in the RSPAN VLAN seen on a source trunk.

The RSPAN traffic from the source ports or source VLANs is switched to the RSPAN VLAN and then forwarded to destination ports, which are in the RSPAN VLAN. The sources (ports or VLANs) in an RSPAN session can be different on different source switches but must be the same for all sources on each RSPAN source switch. Each RSPAN source switch must have either ports or VLANs as RSPAN sources.

Figure 34-2 RSPAN Configuration



Local SPAN and RSPAN Sessions

SPAN sessions (local or remote) allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

A local SPAN session is an association of a set of source ports and source VLANs with one or more destination ports. You configure a local SPAN session on a single network device. Local SPAN does not have separate source and destination sessions.

RSPAN consists of an RSPAN source session, an RSPAN VLAN, and an RSPAN destination session. You separately configure RSPAN source sessions and destination sessions on different network devices. To configure an RSPAN source session on one network device, you associate a set of source ports and VLANs with an RSPAN VLAN. To configure an RSPAN destination session on another device, you associate the destination port with the RSPAN VLAN.

Monitored Traffic

These sections describe the traffic that SPAN (local or remote) can monitor:

- Monitored Traffic Direction, page 34-4
- Monitored Traffic Type, page 34-4
- Duplicate Traffic, page 34-4

Monitored Traffic Direction

You can configure SPAN sessions to monitor ingress network traffic (called ingress SPAN), or to monitor egress network traffic (called egress SPAN), or to monitor traffic flowing in both directions.

Ingress SPAN copies network traffic received by the source ports and VLANs for analysis at the destination port. Egress SPAN copies network traffic transmitted from the source ports and VLANs. When you enter the **both** keyword, SPAN copies the network traffic received and transmitted by the source ports and VLANs to the destination port.

Monitored Traffic Type

By default, local SPAN monitors all network traffic, including multicast and bridge protocol data unit (BPDU) frames. RSPAN does not support BPDU monitoring.

Duplicate Traffic

In some configurations, SPAN sends multiple copies of the same source traffic to the destination port. For example, in a configuration with a bidirectional SPAN session (both ingress and egress) for two SPAN sources, called s1 and s2, to a SPAN destination port, called d1, if a packet enters the switch through s1 and is sent for egress from the switch to s2, ingress SPAN at s1 sends a copy of the packet to SPAN destination d1 and egress SPAN at s2 sends a copy of the packet to SPAN destination d1. If the packet was Layer 2 switched from s1 to s2, both SPAN packets would be the same. If the packet was Layer 3 switched from s1 to s2, the Layer-3 rewrite would alter the source and destination Layer 2 addresses, in which case the SPAN packets would be different.

SPAN Sources

These sections describe local SPAN and RSPAN sources:

- Source Ports, page 34-4
- Source VLANs, pagc 34-5

Source Ports

A source port is a port monitored for network traffic analysis. You can configure both switched and routed ports as SPAN source ports. SPAN can monitor one or more source ports in a single SPAN session. You can configure source ports in any VLAN. Trunk ports can be configured as source ports and mixed with nontrunk source ports, but SPAN does not copy the encapsulation from a source trunk port.

Source VLANs

A source VLAN is a VLAN monitored for network traffic analysis. VLAN-based SPAN (VSPAN) uses a VLAN as the SPAN source. All the ports in the source VLANs become source ports.

Destination Ports

A destination port is a Layer 2 or Layer 3 LAN port to which SPAN sends traffic for analysis.

When you configure a port as a SPAN destination port, it can no longer receive any traffic. When you configure a port as a SPAN destination port, the port is dedicated for use only by the SPAN feature. A SPAN destination port does not forward any traffic except that required for the SPAN session.

With Release 12.1(13)E and later releases, you can configure trunk ports as destination ports, which allows destination trunk ports to transmit encapsulated traffic. With earlier releases, trunk ports stop trunking when you configure them as a destination port.

Local SPAN and RSPAN Configuration Guidelines and Restrictions

These sections describe local SPAN and RSPAN configuration guidelines and restrictions:

- Local SPAN and RSPAN Session Limits, page 34-5
- Local SPAN and RSPAN Source and Destination Limits, page 34-6
- Local SPAN and RSPAN Guidelines and Restrictions, page 34-6
- VSPAN Guidelines and Restrictions, page 34-7
- RSPAN Guidelines and Restrictions, page 34-7

Note

- Release 12.1(13)E and later releases support RSPAN.
- Ports on the WS-X6548-GE-TX and WS-X6548V-GE-TX switching modules cannot be ingress SPAN sources when the switch is operating in truncated mode.

Local SPAN and RSPAN Session Limits

These are the local SPAN and RSPAN session limits:

Total Sessions per Switch	Local SPAN Sessions	RSPAN Source Sessions	RSPAN Destination Sessions
66	2 (ingress or egress or both)	0	64
	1 ingress	1 (ingress or egress or both)	
	1 or 2 egress	0	

Local SPAN and RSPAN Source and Destination Limits

These are the local SPAN and RSPAN source and destination limits:

Sources and Destinations	Local SPAN Sessions	RSPAN Source Sessions	RSPAN Destination Sessions
Egress sources	1 (0 with a remote SPAN source session configured)	1 (0 with a local SPAN egress source session configured)	1 RSPAN VLAN
Ingress sources	64	64	
Destinations per session	64	1 RSPAN VLAN	64

Local SPAN and RSPAN Guidelines and Restrictions

These guidelines and restrictions apply to both local SPAN and RSPAN:

- You need a network analyzer to monitor destination ports.
- You can configure both Layer 2 LAN ports (LAN ports configured with the **switchport** command) and Layer 3 LAN ports (LAN ports not configured with the **switchport** command) as sources or destinations.
- With Release 12.1(13)E and later releases, you can configure destination ports as trunks to capture tagged traffic. With earlier releases, if you configure a trunk port as a destination port, SPAN suspends trunking on the port.
- A port specified as a destination port in one SPAN session cannot be a destination port for another SPAN session.
- A port configured as a destination port cannot be configured as a source port.
- A port channel interface (an EtherChannel) can be a source.
  - With Release 12.1(13)E and later releases, you cannot configure active member ports of an EtherChannel as source ports. Inactive member ports of an EtherChannel can be configured as sources but they are put into the suspended state and carry no traffic.
  - With releases earlier than 12.1(13)E, if you configure a member port of an EtherChannel as a SPAN source port, it is put into the suspended state and carries no traffic.
- A port channel interface (an EtherChannel) cannot be a destination.
  - With Release 12.1(13)E and later releases, you cannot configure active member ports of an EtherChannel as destination ports. Inactive member ports of an EtherChannel can be configured as destinations but they are put into the suspended state and carry no traffic.
  - With releases earlier than 12.1(13)E, if you configure a member port of an EtherChannel as a SPAN destination port, it is put into the suspended state and carries no traffic.
- You cannot mix individual source ports and source VLANs within a single session.
- If you specify multiple ingress source ports, the ports can belong to different VLANs.
- You cannot mix source VLANs and filter VLANs within a session. You can have source VLANs or filter VLANs, but not both at the same time.
- When enabled, local SPAN or RSPAN uses any previously entered configuration.
- When you specify sources and do not specify a traffic direction (ingress, egress, or both), "both" is used by default.

- You cannot configure destination ports to receive ingress traffic.
- Destination ports never participate in any spanning tree instance. Local SPAN includes BPDUs in the monitored traffic, so any BPDUs seen on the destination port are from the source port. RSPAN does not support BPDU monitoring.
- All packets sent through the switch for transmission from a port configured as an egress source are copied to the destination port, including packets that do not exit the switch through the port because STP has put the port into the blocking state, or on a trunk port because STP has put the VLAN into the blocking state on the trunk port.

VSPAN Guidelines and Restrictions

These are VSPAN guidelines and restrictions:

- For VSPAN sessions with both ingress and egress configured, two packets are forwarded from the destination port if the packets get switched on the same VLAN (one as ingress traffic from the ingress port and one as egress traffic from the egress port).
- VSPAN only monitors traffic that leaves or enters Layer 2 ports in the VLAN.
  - If you configure a VLAN as an ingress source and traffic gets routed into the monitored VLAN, the routed traffic is not monitored because it never appears as ingress traffic entering a Layer 2 port in the VLAN.
  - If you configure a VLAN as an egress source and traffic gets routed out of the monitored VLAN, the routed traffic is not monitored because it never appears as egress traffic leaving a Layer 2 port in the VLAN.

RSPAN Guidelines and Restrictions

These are RSPAN guidelines and restrictions:

- Any network device that supports RSPAN VLANs can be an RSPAN intermediate device.
- Networks impose no limit on the number of RSPAN VLANs that the networks carry.
- Intermediate switches might impose limits on the number of RSPAN VLANs that they can support.
- You must configure the RSPAN VLANs in all source, intermediate, and destination network devices. If enabled, the VLAN Trunking Protocol (VTP) can propagate configuration of VLANs numbered 1 through 1024 as RSPAN VLANs. You must manually configure VLANs numbered higher than 1024 as RSPAN VLANs on all source, intermediate, and destination network devices.
- If you enable VTP and VTP pruning, RSPAN traffic is pruned in the trunks to prevent the unwanted flooding of RSPAN traffic across the network.
- RSPAN VLANs can be used only for RSPAN traffic.
- Do not configure a VLAN used to carry management traffic as an RSPAN VLAN.
- Do not assign access ports to RSPAN VLANs. RSPAN puts access ports in an RSPAN VLAN into the suspended state.
- Do not configure any ports in an RSPAN VLAN except those selected to carry RSPAN traffic.
- MAC address learning is disabled on the RSPAN VLAN.
- You can use an output access control list (ACL) on the RSPAN VLAN in the RSPAN source switch to filter the traffic sent to an RSPAN destination.

- RSPAN does not support BPDU monitoring.
- Do not configure RSPAN VLANs as sources in VSPAN sessions.
- You can configure any VLAN as an RSPAN VLAN as long as all participating network devices support configuration of RSPAN VLANs and you use the same RSPAN VLAN for each RSPAN session in all participating network devices.
- Entering SPAN configuration commands does not clear previously configured SPAN parameters. You must enter the **no monitor session** command to clear configured SPAN parameters.

Configuring Local SPAN and RSPAN

These sections describe how to configure local SPAN and RSPAN:

- Local SPAN and RSPAN Configuration Overview, page 34-8
- Configuring RSPAN VLANs, page 34-8
- Configuring Local or RSPAN Sources, page 34-9
- Monitoring Specific Source VLANs on a Source Trunk Port, page 34-10
- Configuring Local SPAN and RSPAN Destinations, page 34-10
- Verifying the Configuration, page 34-12
- Configuration Examples, page 34-12

Note With Release 12.1(11b)E and later releases, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

Local SPAN and RSPAN Configuration Overview

To configure a local SPAN session, use the same session number for the sources and the destination ports.

To configure an RSPAN source session, use the same session number for a source and a destination RSPAN VLAN.

To configure an RSPAN destination session, use the same session number for a source RSPAN VLAN and a destination port.

Configuring RSPAN VLANs

To configure a VLAN as an RSPAN VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# **vlan** *vlan_ID*{[-*vlan_ID*]|[,*vlan_ID*])`	Creates or modifies an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs specified in a comma-separated list (do not enter space characters).

	Command	Purpose
Step 2	Router(config-vlan)# **remote-span**	Configures the VLAN as an RSPAN VLAN.
	Router(config-vlan)# **no remote-span**	Clears the RSPAN VLAN configuration.
Step 3	Router(config-vlan)# **end**	Updates the VLAN database and returns to privileged EXEC mode.

Configuring Local or RSPAN Sources

Note To configure an RSPAN source session, configure a source with an RSPAN VLAN as the destination. To configure an RSPAN destination session, configure an RSPAN VLAN as the source and a port as the destination.

To configure a local SPAN or RSPAN source, perform this task:

Command	Purpose
Router(config)# **monitor session** *session_number* **source** {{*single_interface* | *interface_list* | *interface_range* | *mixed_interface_list* | *single_vlan* | *vlan_list* | *vlan_range* | *mixed_vlan_list*} [**rx** | **tx** | **both**]} | {**remote vlan** *rspan_vlan_ID*}}	Configures the session number, the source ports, VLANs, or RSPAN VLAN, and the traffic direction to be monitored.
Router(config)# **no monitor session** {*session_number* | **all** | **local** | **range** *session_range*[,*session_range*],...] | **remote**}	Clears the monitor configuration.

When configuring monitor sessions, note the following syntax information:

- *single_interface* is **interface** *type slot/port*; *type* is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- *interface_list* is *single_interface* , *single_interface* , *single_interface* ...

Note In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface_range* is **interface** *type slot/first_port - last_port*
- *mixed_interface_list* is, in any order, *single_interface* , *interface_range* , ...
- *single_vlan* is a the ID number of a single VLAN.
- *vlan_list* is *single_vlan* , *single_vlan* , *single_vlan* ...
- *vlan_range* is *first_vlan_ID - last_vlan_ID*
- *mixed_vlan_list* is, in any order, *single_vlan* , *vlan_range* , ...

When clearing monitor sessions, note the following syntax information:

- The **no monitor session** *number* command entered with no other parameters clears session *session_number*.
- *session_range* is *first_session_number-last_session_number*

Note In the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

This example shows how to configure session 1 to monitor bidirectional traffic from Fast Ethernet port 5/1:

```
Router(config)# monitor session 1 source interface fastethernet 5/1
```

Monitoring Specific Source VLANs on a Source Trunk Port

To monitor specific VLANs when the local or RSPAN source is a trunk port, perform this task:

Command	Purpose
`Router(config)# monitor session session_number filter {vlan_ID} [, | -]`	Monitors specific VLANs when the source is a trunk port.
`Router(config)# no monitor session session_number filter {vlan_ID}`	Clears trunk source configuration.

This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the source is a trunk port:

```
Router(config)# monitor session 2 filter vlan 1 - 5 , 9
```

Configuring Local SPAN and RSPAN Destinations

These sections describe how to configure local SPAN and RSPAN destinations:

- Configuring a Destination Port as an Unconditional Trunk, page 34-10
- Configuring a Local or RSPAN Destination, page 34-11

Configuring a Destination Port as an Unconditional Trunk

To tag the monitored traffic with Release 12.1(13)E and later releases, configure the destination port as a trunk.

To configure the destination port as a trunk, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface type[1] slot/port`	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport`	Configures the LAN port for Layer 2 switching (required only if the LAN port is not already configured for Layer 2 switching).
Step 3	`Router(config-if)# switchport trunk encapsulation {isl | dot1q}`	Configures the encapsulation, which configures the Layer 2 switching port as either an ISL or 802.1Q trunk.
Step 4	`Router(config-if)# switchport mode trunk`	Configures the port to trunk unconditionally.
Step 5	`Router(config-if)# switchport nonegotiate`	Configures the trunk not to use DTP.

[1] *type* = **ethernet, fastethernet, gigabitethernet,** or **tengigabitethernet**

This example shows how to configure a port as an unconditional IEEE 802.1q trunk:

```
Router(config)# interface fastethernet 5/12
Router(config-if)# switchport
Router(config-if)# switchport trunk encapsulation dot1q
Router(config-if)# switchport mode trunk
Router(config-if)# switchport nonegotiate
```

Configuring a Local or RSPAN Destination

Note To configure an RSPAN source session, configure a source with an RSPAN VLAN as the destination. To configure an RSPAN destination session, configure an RSPAN VLAN as the source and a port as the destination.

To configure a local or RSPAN destination, perform this task:

Command	Purpose
`Router(config)# monitor session session_number destination {single_interface | interface_list | interface_range | mixed_interface_list} | {remote vlan rspan_vlan_ID}}`	Configures the session number and the destination ports or RSPAN VLAN.
`Router(config)# no monitor session {session_number | all | local | range session_range[[,session_range],...] | remote}`	Clears the monitor configuration.

Note To tag the monitored traffic, you must configure the port to trunk unconditionally before you configure it as a destination (see the "Configuring a Destination Port as an Unconditional Trunk" section on page 34-10).

When configuring monitor sessions, note the following syntax information:

- *single_interface* is **interface** *type slot/port*; *type* is **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
- *interface_list* is *single_interface* , *single_interface* , *single_interface* ...

Note In lists, you must enter a space before and after the comma. In ranges, you must enter a space before and after the dash.

- *interface_range* is **interface** *type slot/first_port - last_port*
- *mixed_interface_list* is, in any order, *single_interface* , *interface_range* , ...

When clearing monitor sessions, note the following syntax information:

- Enter the **no monitor session** *number* command with no other parameters to clear session *session_number*.
- *session_range* is *first_session_number-last_session_number*

Note In the **no monitor session range** command, do not enter spaces before or after the dash. If you enter multiple ranges, do not enter spaces before or after the commas.

This example shows how to configure Fast Ethernet port 5/48 as the destination for SPAN session 1:

```
Router(config)# monitor session 1 destination interface fastethernet 5/48
```

Verifying the Configuration

This example shows how to verify the configuration of session 2:

```
Router# show monitor session 2
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:       Fa3/1
Dest RSPAN VLAN:   901
Router#
```

This example shows how to display the full details of session 2:

```
Router# show monitor session 2 detail
Session 2
------------
Type : Remote Source Session

Source Ports:
    RX Only:       Fa1/1-3
    TX Only:       None
    Both:          None
Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Source RSPAN VLAN: None
Destination Ports: None
Filter VLANs:      None
Dest RSPAN VLAN:   901
```

Configuration Examples

This example shows how to configure RSPAN source session 2:

```
Router(config)# monitor session 2 source interface fastethernet1/1 - 3 rx
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to clear the configuration for sessions 1 and 2:

```
Router(config)# no monitor session range 1-2
```

This example shows how to configure an RSPAN source session with multiple sources:

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

This example shows how to remove sources for a session:

```
Router(config)# no monitor session 2 source interface fastethernet 5/15 , 7/3
```

This example shows how to remove options for sources for a session:

```
Router(config)# no monitor session 2 source interface gigabitethernet 1/2
Router(config)# no monitor session 2 source interface port-channel 102 tx
```

This example shows how to remove VLAN filtering for a session:

```
Router(config)# no monitor session 2 filter vlan 3
```

This example shows how to configure an RSPAN destination session:

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```

CHAPTER 15

Configuring STP and IEEE 802.1s MST

This chapter describes how to configure the Spanning Tree Protocol (STP) and the IEEE 802.1s Multiple Spanning Tree (MST) protocol on Catalyst 6500 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

Note

- For information on configuring the PortFast, UplinkFast, and BackboneFast STP enhancements, see Chapter 16, “Configuring Optional STP Features.”
- Release 12.1(13)E and later releases support IEEE 802.1s MST and IEEE 802.1w, rapid reconfiguration of spanning tree.

Understanding How STP Works

These sections describe how STP works:

- STP Overview, page 15-2
- Understanding the Bridge ID, page 15-3
- Understanding Bridge Protocol Data Units, page 15-4
- Election of the Root Bridge, page 15-4
- STP Protocol Timers, page 15-5
- Creating the Spanning Tree Topology, page 15-5
- STP Port States, page 15-6
- STP and IEEE 802.1Q Trunks, page 15-12

STP Overview

STP is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. STP operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

Catalyst 6500 series switches use STP (the IEEE 802.1D bridge protocol) on all VLANs. By default, a single instance of STP runs on each configured VLAN (provided you do not manually disable STP). You can enable and disable STP on a per-VLAN basis.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The STP algorithm calculates the best loop-free path throughout a switched Layer 2 network. Layer 2 LAN ports send and receive STP frames at regular intervals. Network devices do not forward these frames, but use the frames to construct a loop-free path.

Multiple active paths between end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages and network devices might learn end station MAC addresses on multiple Layer 2 LAN ports. These conditions result in an unstable network.

STP defines a tree with a root bridge and a loop-free path from the root to all network devices in the Layer 2 network. STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the STP algorithm recalculates the spanning tree topology and activates the standby path.

When two Layer 2 LAN ports on a network device are part of a loop, the STP port priority and port path cost setting determine which port is put in the forwarding state and which port is put in the blocking state. The STP port priority value represents the location of a port in the network topology and how well located it is to pass traffic. The STP port path cost value represents media speed.

Understanding the Bridge ID

Each VLAN on each network device has a unique 64-bit bridge ID consisting of a bridge priority value, an extended system ID, and an STP MAC address allocation.

This section contains these topics:

- Bridge Priority Value, page 15-3
- Extended System ID, page 15-3
- STP MAC Address Allocation, page 15-3

Bridge Priority Value

With Release 12.1(8a)E and later releases, the bridge priority is a 4-bit value when the extended system ID is enabled (see Table 15-2 on page 15-3). With earlier releases, the bridge priority is a 16-bit value (see Table 15-1 on page 15-3). See the "Configuring the Bridge Priority of a VLAN" section on page 15-30.

Extended System ID

Release 12.1(8a)E and later releases support a 12-bit extended system ID field as part of the bridge ID (see Table 15-2 on page 15-3). Chassis that support only 64 MAC addresses always use the 12-bit extended system ID. On chassis that support 1024 MAC addresses, you can enable use of the extended system ID. STP uses the VLAN ID as the extended system ID. See the "Enabling the Extended System ID" section on page 15-24.

Table 15-1 Bridge Priority Value with the Extended System ID Disabled

Bridge Priority Value															
Bit 16	**Bit 15**	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Table 15-2 Bridge Priority Value and Extended System ID with the Extended System ID Enabled

Bridge Priority Value				Extended System ID (Set Equal to the VLAN ID)											
Bit 16	**Bit 15**	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

STP MAC Address Allocation

Catalyst 6500 series switch chassis have either 64 or 1024 MAC addresses available to support software features such as STP. To view the MAC address range on your chassis, enter the **show catalyst6000 chassis-mac-address** command.

Release 12.1(8a)E and later releases support chassis with 64 or 1024 MAC addresses. For chassis with 64 MAC addresses, STP uses the extended system ID plus a MAC address to make the bridge ID unique for each VLAN.

Earlier releases support chassis with 1024 MAC addresses. With earlier releases, STP uses one MAC address per VLAN to make the bridge ID unique for each VLAN.

If you have a network device in your network with MAC address reduction enabled, you should also enable MAC address reduction on all other Layer-2 connected network devices to avoid undesirable root bridge election and spanning tree topology issues.

When MAC address reduction is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. With MAC address reduction enabled, a switch bridge ID (used by the spanning-tree algorithm to determine the identity of the root bridge, the lowest being preferred) can only be specified as a multiple of 4096. Only the following values are possible: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

If another bridge in the same spanning-tree domain does not run the MAC address reduction feature, it could win root bridge ownership because of the finer granularity in the selection of its bridge ID.

Understanding Bridge Protocol Data Units

Bridge protocol data units (BPDUs) are transmitted in one direction from the root bridge. Each network device sends configuration BPDUs to communicate and compute the spanning tree topology. Each configuration BPDU contains the following minimal information:

- The unique bridge ID of the network device that the transmitting network device believes to be tł root bridge
- The STP path cost to the root
- The bridge ID of the transmitting bridge
- Message age
- The identifier of the transmitting port
- Values for the hello, forward delay, and max-age protocol timers

When a network device transmits a BPDU frame, all network devices connected to the LAN on which the frame is transmitted receive the BPDU. When a network device receives a BPDU, it does not forward the frame but instead uses the information in the frame to calculate a BPDU, and, if the topology changes, initiate a BPDU transmission.

A BPDU exchange results in the following:

- One network device is elected as the root bridge.
- The shortest distance to the root bridge is calculated for each network device based on the path cost.
- A designated bridge for each LAN segment is selected. This is the network device closest to the root bridge through which frames are forwarded to the root.
- A root port is selected. This is the port providing the best path from the bridge to the root bridge.
- Ports included in the spanning tree are selected.

Election of the Root Bridge

For each VLAN, the network device with the highest bridge ID (the lowest numerical ID value) is elected as the root bridge. If all network devices are configured with the default priority (32768), the network device with the lowest MAC address in the VLAN becomes the root bridge. The bridge priority value occupies the most significant bits of the bridge ID.

When you change the bridge priority value, you change the probability that the switch will be elected as the root bridge. Configuring a higher value increases the probability; a lower value decreases the probability.

The STP root bridge is the logical center of the spanning tree topology in a Layer 2 network. All paths that are not needed to reach the root bridge from anywhere in the Layer 2 network are placed in STP blocking mode.

BPDUs contain information about the transmitting bridge and its ports, including bridge and MAC addresses, bridge priority, port priority, and path cost. STP uses this information to elect the root bridge for the Layer 2 network, to elect the root port leading to the root bridge, and to determine the designated port for each Layer 2 segment.

STP Protocol Timers

Table 15-3 describes the STP protocol timers that affect STP performance.

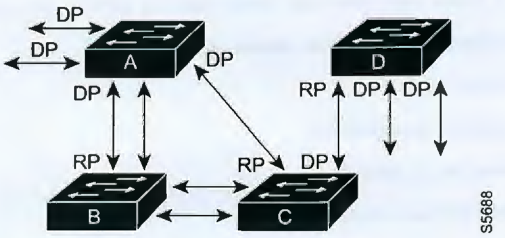
Table 15-3 STP Protocol Timers

Variable	Description
Hello timer	Determines how often the network device broadcasts hello messages to other network devices.
Forward delay timer	Determines how long each of the listening and learning states last before the port begins forwarding.
Maximum age timer	Determines the amount of time protocol information received on an port is stored by the network device.

Creating the Spanning Tree Topology

In Figure 15-1, Switch A is elected as the root bridge because the bridge priority of all the network devices is set to the default (32768) and Switch A has the lowest MAC address. However, due to traffic patterns, number of forwarding ports, or link types, Switch A might not be the ideal root bridge. By increasing the priority (lowering the numerical value) of the ideal network device so that it becomes the root bridge, you force an STP recalculation to form a new spanning tree topology with the ideal network device as the root.

Figure 15-1 Spanning Tree Topology



RP = Root Port
DP = Designated Port

When the spanning tree topology is calculated based on default parameters, the path between source and destination end stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change. The goal is to make the fastest link the root port.

For example, assume that one port on Switch B is a fiber-optic link, and another port on Switch B (an unshielded twisted-pair [UTP] link) is the root port. Network traffic might be more efficient over the high-speed fiber-optic link. By changing the STP port priority on the fiber-optic port to a higher priority (lower numerical value) than the root port, the fiber-optic port becomes the new root port.

STP Port States

These sections describe the STP port states:

- STP Port State Overview, page 15-6
- Blocking State, page 15-8
- Listening State, page 15-9
- Learning State, page 15-10
- Forwarding State, page 15-11
- Disabled State, page 15-12

STP Port State Overview

Propagation delays can occur when protocol information passes through a switched LAN. As a result, topology changes can take place at different times and at different places in a switched network. When a Layer 2 LAN port transitions directly from nonparticipation in the spanning tree topology to the forwarding state, it can create temporary data loops. Ports must wait for new topology information to propagate through the switched LAN before starting to forward frames. They must allow the frame lifetime to expire for frames that have been forwarded using the old topology.

Each Layer 2 LAN port on a Catalyst 6500 series switch using STP exists in one of the following five states:

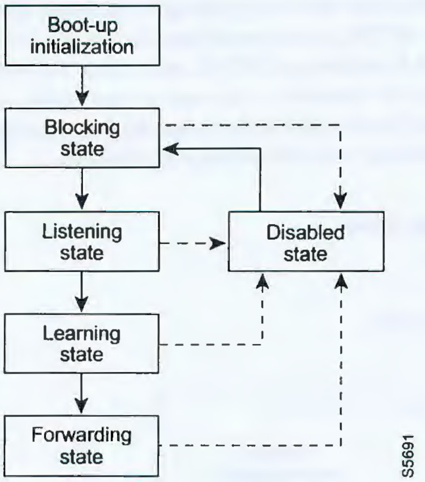
- Blocking—The Layer 2 LAN port does not participate in frame forwarding.
- Listening—First transitional state after the blocking state when STP determines that the Layer 2 LAN port should participate in frame forwarding.
- Learning—The Layer 2 LAN port prepares to participate in frame forwarding.
- Forwarding—The Layer 2 LAN port forwards frames.
- Disabled—The Layer 2 LAN port does not participate in STP and is not forwarding frames.

A Layer 2 LAN port moves through these five states as follows:

- From initialization to blocking
- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

Figure 15-2 illustrates how a Layer 2 LAN port moves through the five states.

Figure 15-2 STP Layer 2 LAN Interface States



When you enable STP, every port in the Catalyst 6500 series switch, VLAN, and network goes through the blocking state and the transitory states of listening and learning at power up. If properly configured, each Layer 2 LAN port stabilizes to the forwarding or blocking state.

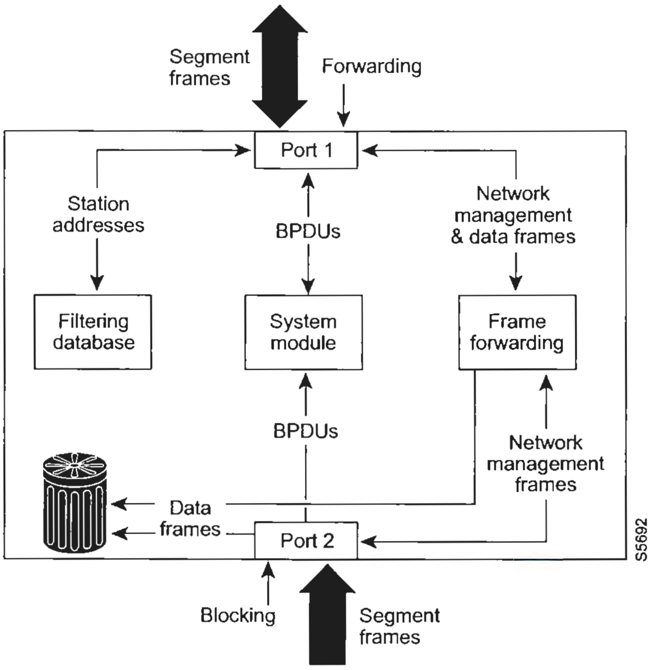
When the STP algorithm places a Layer 2 LAN port in the forwarding state, the following process occurs:

1. The Layer 2 LAN port is put into the listening state while it waits for protocol information that suggests it should go to the blocking state.
2. The Layer 2 LAN port waits for the forward delay timer to expire, moves the Layer 2 LAN port to the learning state, and resets the forward delay timer.
3. In the learning state, the Layer 2 LAN port continues to block frame forwarding as it learns end station location information for the forwarding database.
4. The Layer 2 LAN port waits for the forward delay timer to expire and then moves the Layer 2 LAN port to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

A Layer 2 LAN port in the blocking state does not participate in frame forwarding, as shown in Figure 15-3. After initialization, a BPDU is sent out to each Layer 2 LAN port. A network device initially assumes it is the root until it exchanges BPDUs with other network devices. This exchange establishes which network device in the network is the root or root bridge. If only one network device is in the network, no exchange occurs, the forward delay timer expires, and the ports move to the listening state. A port always enters the blocking state following initialization.

Figure 15-3 Interface 2 in Blocking State



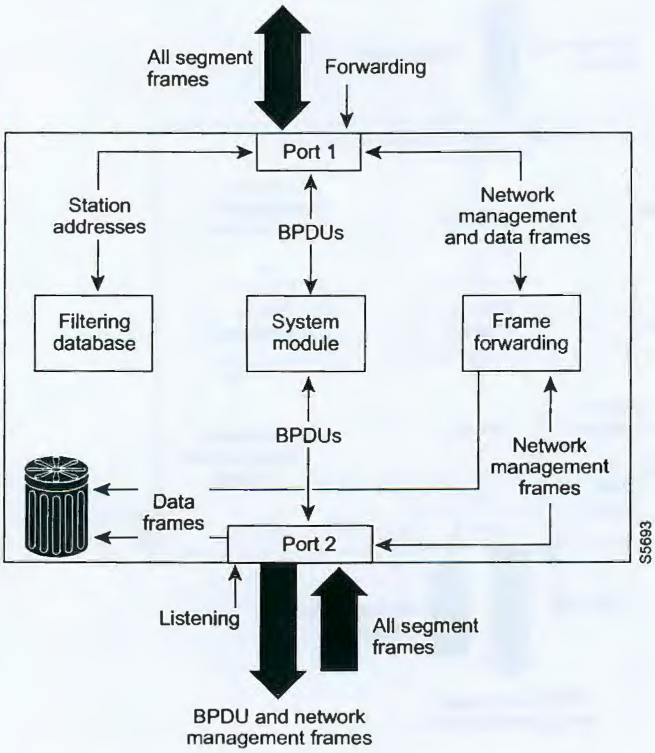
A Layer 2 LAN port in the blocking state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate end station location into its address database. (There is no learning on a blocking Layer 2 LAN port, so there is no address database update.)
- Receives BPDUs and directs them to the system module.
- Does not transmit BPDUs received from the system module.
- Receives and responds to network management messages.

Listening State

The listening state is the first transitional state a Layer 2 LAN port enters after the blocking state. The Layer 2 LAN port enters this state when STP determines that the Layer 2 LAN port should participate in frame forwarding. Figure 15-4 shows a Layer 2 LAN port in the listening state.

Figure 15-4 Interface 2 in Listening State



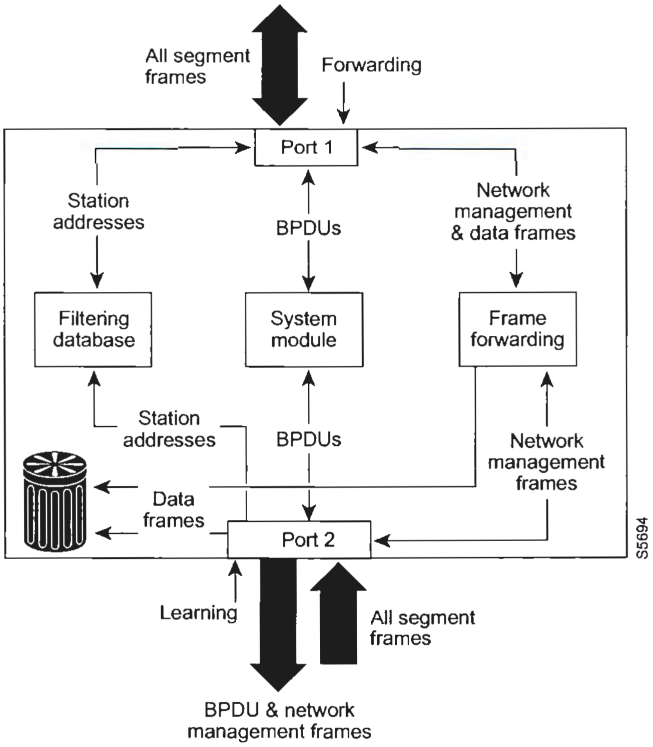
A Layer 2 LAN port in the listening state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another LAN port for forwarding.
- Does not incorporate end station location into its address database. (There is no learning at this point, so there is no address database update.)
- Receives BPDUs and directs them to the system module.
- Receives, processes, and transmits BPDUs received from the system module.
- Receives and responds to network management messages.

Learning State

A Layer 2 LAN port in the learning state prepares to participate in frame forwarding. The Layer 2 LAN port enters the learning state from the listening state. Figure 15-5 shows a Layer 2 LAN port in the learning state.

Figure 15-5 Interface 2 in Learning State



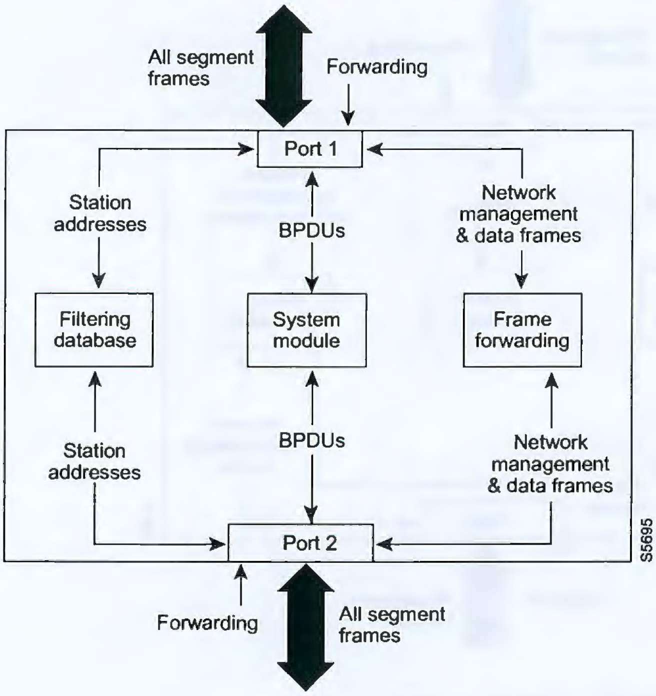
A Layer 2 LAN port in the learning state performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Incorporates end station location into its address database.
- Receives BPDUs and directs them to the system module.
- Receives, processes, and transmits BPDUs received from the system module.
- Receives and responds to network management messages.

Forwarding State

A Layer 2 LAN port in the forwarding state forwards frames, as shown in Figure 15-6. The Layer 2 LAN port enters the forwarding state from the learning state.

Figure 15-6 Interface 2 in Forwarding State



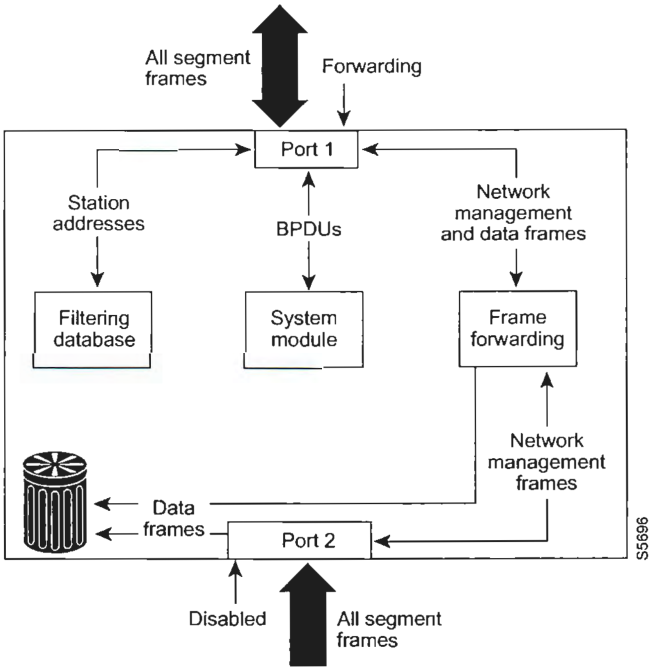
A Layer 2 LAN port in the forwarding state performs as follows:

- Forwards frames received from the attached segment.
- Forwards frames switched from another port for forwarding.
- Incorporates end station location information into its address database.
- Receives BPDUs and directs them to the system module.
- Processes BPDUs received from the system module.
- Receives and responds to network management messages.

Disabled State

A Layer 2 LAN port in the disabled state does not participate in frame forwarding or STP, as shown in Figure 15-7. A Layer 2 LAN port in the disabled state is virtually nonoperational.

Figure 15-7 Interface 2 in Disabled State



A disabled Layer 2 LAN port performs as follows:

- Discards frames received from the attached segment.
- Discards frames switched from another port for forwarding.
- Does not incorporate end station location into its address database. (There is no learning, so there is no address database update.)
- Does not receive BPDUs.
- Does not receive BPDUs for transmission from the system module.

STP and IEEE 802.1Q Trunks

802.1Q trunks impose some limitations on the STP strategy for a network. In a network of Cisco network devices connected through 802.1Q trunks, the network devices maintain one instance of STP for each VLAN allowed on the trunks. However, non-Cisco 802.1Q network devices maintain only one instance of STP for all VLANs allowed on the trunks.

When you connect a Cisco network device to a non-Cisco device through an 802.1Q trunk, the Cisco network device combines the STP instance of the 802.1Q VLAN of the trunk with the STP instance of the non-Cisco 802.1Q network device. However, all per-VLAN STP information is maintained by Cisco network devices separated by a cloud of non-Cisco 802.1Q network devices. The non-Cisco 802.1Q cloud separating the Cisco network devices is treated as a single trunk link between the network devices.

For more information on 802.1Q trunks, see Chapter 7, "Configuring LAN Ports for Layer 2 Switching."

Understanding How IEEE 802.1w RSTP Works

Note In Cisco IOS release 12.1(11)EX and later releases, RSTP is implemented as part of Multiple Spanning Tree Protocol (MSTP). In Cisco IOS release 12.1(13)E and later releases, RSTP is also available as a standalone protocol in Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) mode. In this mode, the switch runs an RSTP instance on each VLAN, which follows the usual PVST+ approach.

These sections describe Rapid Spanning Tree Protocol (RSTP):

- IEEE 802.1w RSTP Overview, page 15-13
- RSTP Port Roles, page 15-13
- RSTP Port States, page 15-14
- Rapid-PVST, page 15-14

IEEE 802.1w RSTP Overview

RSTP significantly reduces the time to reconfigure the active topology of the network when changes occur to the physical topology or its configuration parameters. RSTP selects one switch as the root of a spanning tree-connected active topology and assigns port roles to individual ports of the switch, depending on whether that port is part of the active topology.

RSTP provides rapid connectivity following the failure of a switch, switch port, or a LAN. A new root port and the designated port on the other side of the bridge transition to forwarding using an explicit handshake between them. RSTP allows switch port configuration so that the ports can transition to forwarding directly when the switch reinitializes.

RSTP as specified in 802.1w supersedes STP specified in 802.1D, but remains compatible with STP.

RSTP provides backward compatibility with 802.1D bridges as follows:

- RSTP selectively sends 802.1D-configured BPDUs and topology change notification (TCN) BPDUs on a per-port basis.
- When a port initializes, the migration-delay timer starts and RSTP BPDUs are transmitted. While the migration-delay timer is active, the bridge processes all BPDUs received on that port.
- If the bridge receives an 802.1D BPDU after a port's migration-delay timer expires, the bridge assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- When RSTP uses 802.1D BPDUs on a port and receives an RSTP BPDU after the migration-delay expires, RSTP restarts the migration-delay timer and begins using RSTP BPDUs on that port.

RSTP Port Roles

RSTP uses the following definitions for port roles:

- Root—A forwarding port elected for the spanning tree topology.
- Designated—A forwarding port elected for every switched LAN segment.
- Alternate—An alternate path to the root bridge to that provided by the current root port.

- Backup—A backup for the path provided by a designated port toward the leaves of the spanning tree. Backup ports can exist only where two ports are connected together in a loopback by a point-to-point link or bridge with two or more connections to a shared LAN segment.
- Disabled—A port that has no role within the operation of spanning tree.

Port roles are assigned as follows:

- A root port or designated port role includes the port in the active topology.
- An alternate port or backup port role excludes the port from the active topology.

RSTP Port States

The port state controls the forwarding and learning processes and provides the values of discarding, learning, and forwarding. Table 15-4 provides a comparison between STP port states and RSTP port states.

Table 15-4 Comparison Between STP and RSTP Port States

Operational Status	STP Port State	RSTP Port State	Port Included in Active Topology
Enabled	Blocking[1]	Discarding[2]	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

[1] IEEE 802.1D port state designation.

[2] IEEE 802.1w port state designation. Discarding is the same as blocking in RSTP and MST.

In a stable topology, RSTP ensures that every root port and designated port transition to forwarding, and ensures that all alternate ports and backup ports are always in the discarding state.

Rapid-PVST

Rapid-PVST uses the existing configuration for PVST+; however, Rapid-PVST uses RSTP to provide faster convergence. Independent VLANs run their own RSTP instance.

Dynamic entries are flushed immediately on a per-port basis upon receiving a topology change.

UplinkFast and BackboneFast configurations are ignored in Rapid-PVST mode; both features are included in RSTP.

Understanding How IEEE 802.1s MST Works

Note In Cisco IOS release 12.1(11)EX and later releases, RSTP is implemented as part of Multiple Spanning Tree Protocol (MSTP). In Cisco IOS release 12.1(13)E and later releases, RSTP is also available as a standalone protocol in Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) mode. In this mode, the switch runs an RSTP instance on each VLAN, which follows the usual PVST+ approach.

These sections describe Multiple Spanning Tree (MST):

- IEEE 802.1s MST Overview, page 15-15
- MST-to-PVST Interoperability, page 15-16
- Common Spanning Tree, page 15-18
- MST Instances, page 15-18
- MST Configuration Parameters, page 15-18
- MST Regions, page 15-19
- Message Age and Hop Count, page 15-20
- Default STP Configuration, page 15-21

IEEE 802.1s MST Overview

Releases 12.1(11b)EX and later releases support MST. MST in this release is based on the draft version of the IEEE standard. 802.1s for MST is an amendment to 802.1Q. MST extends the IEEE 802.1w rapid spanning tree (RST) algorithm to multiple spanning trees. This extension provides both rapid convergence and load balancing in a VLAN environment. MST converges faster than PVST+. MST is backward compatible with 802.1D STP, 802.1w (rapid spanning tree protocol [RSTP]), and the Cisco PVST+ architecture.

MST allows you to build multiple spanning trees over trunks. You can group and associate VLANs to spanning tree instances. Each instance can have a topology independent of other spanning tree instances. This new architecture provides multiple forwarding paths for data traffic and enables load balancing. Network fault tolerance is improved because a failure in one instance (forwarding path) does not affect other instances (forwarding paths).

In large networks, you can more easily administer the network and use redundant paths by locating different VLAN and spanning tree instance assignments in different parts of the network. A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments. You must configure a set of bridges with the same MST configuration information, which allows them to participate in a specific set of spanning tree instances. Interconnected bridges that have the same MST configuration are referred to as an *MST region*.

MST uses the modified RSTP version called the Multiple Spanning Tree Protocol (MSTP). The MST feature has these characteristics:

- MST runs a variant of spanning tree called internal spanning tree (IST). IST augments the common spanning tree (CST) information with internal information about the MST region. The MST region appears as a single bridge to adjacent single spanning tree (SST) and MST regions.
- A bridge running MST provides interoperability with single spanning tree bridges as follows:
  - MST bridges run IST, which augments the common spanning tree (CST) information with internal information about the MST region.
  - IST connects all the MST bridges in the region and appears as a subtree in the CST that includes the whole bridged domain. The MST region appears as a virtual bridge to adjacent SST bridges and MST regions.
  - The common and internal spanning tree (CIST) is the collection of ISTs in each MST region, the CST that interconnects the MST regions, and the SST bridges. CIST is the same as an IST inside an MST region and the same as CST outside an MST region. The STP, RSTP, and MSTP together elect a single bridge as the root of the CIST.

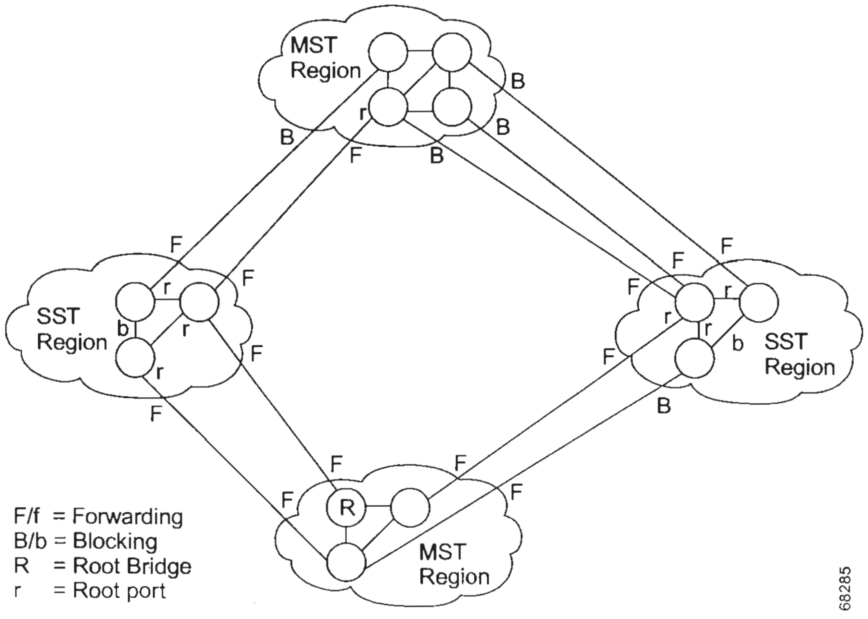
- MST establishes and maintains additional spanning trees within each MST region. These spanning trees are referred to as MST instances (MSTIs). The IST is numbered 0, and the MSTIs are numbered 1,2,3, and so on. Any MSTI is local to the MST region that is independent of MSTIs in another region, even if the MST regions are interconnected. MST instances combine with the IST at the boundary of MST regions to become the CST as follows:
  - Spanning tree information for an MSTI is contained in an MSTP record (M-record).

    M-records are always encapsulated within MST BPDUs (MST BPDUs). The original spanning trees computed by MSTP are called M-trees. M-trees are active only within the MST region. M-trees merge with the IST at the boundary of the MST region and form the CST.
- MST provides interoperability with PVST+ by generating PVST+ BPDUs for the non-CST VLANs.
- MST supports some of the PVST+ extensions in MSTP as follows:
  - UplinkFast and BackboneFast are not available in MST mode; they are included in RSTP.
  - PortFast is supported.
  - BPDU filter and BPDU guard are supported in MST mode.
  - Loop guard and root guard are supported in MST. MST preserves the VLAN 1 disabled functionality except that BPDUs are still transmitted in VLAN 1.
  - MST switches operate as if MAC reduction is enabled.
  - For private VLANs (PVLANs), secondary VLANs must be mapped to the same instance as the primary.

MST-to-PVST Interoperability

A virtual bridged LAN may contain interconnected regions of single spanning tree (SST) and MST bridges. Figure 15-8 shows this relationship.

Figure 15-8 Network with Interconnected SST and MST Regions



An MST region appears as an SST or pseudobridge to STP running in the SST region. Pseudobridges operate as follows:

- The same values for root identifiers and root path costs are sent in all BPDUs of all the pseudobridge ports. Pseudobridges differ from a single SST bridge as follows:
  - The pseudobridge BPDUs have different bridge identifiers. This difference does not affect STP operation in the neighboring SST regions because the root identifier and root cost are the same.
  - BPDUs sent from the pseudobridge ports may have significantly different message ages. Because the message age increases by 1 second for each hop, the difference in the message age is in the order of seconds.
- Data traffic from one port of a pseudobridge (a port at the edge of a region) to another port follows a path entirely contained within the pseudobridge or MST region.
- Data traffic belonging to different VLANs may follow different paths within the MST regions established by MST.
- Loop prevention is achieved by either of the following:
  - Blocking the appropriate pseudobridge ports by allowing one forwarding port on the boundary and blocking all other ports.
  - Setting the CST partitions to block the ports of the SST regions.
- A pseudobridge differs from a single SST bridge because the BPDUs sent from the pseudobridge's ports have different bridge identifiers. The root identifier and root cost are the same for both bridges.

These guidelines apply in a topology where you configure MST switches (all in the same region) to interact with PVST+ switches:

- Configure the root for all VLANs inside the MST region as shown in this example:

```
Router# show spanning-tree mst interface gigabitethernet 1/1

GigabitEthernet1/1 of MST00 is root forwarding
Edge port: no              (trunk)          port guard : none        (default)
Link type: point-to-point  (auto)           bpdu filter: disable     (default)
Boundary : boundary        (PVST)           bpdu guard : disable     (default)
Bpdus sent 10, received 310

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- -------------------------------
0        Root FWD 20000     128.1    1-2,4-2999,4000-4094
3        Boun FWD 20000     128.1    3,3000-3999
```

  The ports that belong to the MST switch at the boundary simulate PVST+ and send PVST+ BPDUs for all the VLANs.

  If you enable loop guard on the PVST+ switches, the ports might change to a loop-inconsistent state when the MST switches change their configuration. To correct the loop-inconsistent state, you must disable and reenable loop guard on that PVST+ switch.

- Do not locate the root for some or all of the VLANs inside the PVST+ side of the MST switch because when the MST switch at the boundary receives PVST+ BPDUs for all or some of the VLANs on its designated ports, root guard sets the port to the blocking state. Do not designate switches with a slower CPU running PVST+ as a switch running MST.

When you connect a PVST+ switch to two different MST regions, the topology change from the PVST+ switch does not pass beyond the first MST region. In this case, the topology changes are only propagated in the instance to which the VLAN is mapped. The topology change stays local to the first MST region and the CAM entries in the other region are not flushed. To make the topology change visible throughout other MST regions, you can map that VLAN to IST or connect the PVST+ switch to the two regions through access links.

Common Spanning Tree

CST (802.1Q) is a single spanning tree for all the VLANs. In a Catalyst 6000 family switch running PVST+, the VLAN 1 spanning tree corresponds to CST. In a Catalyst 6000 family switch running MST, IST (instance 0) corresponds to CST.

MST Instances

This release supports up to 16 instances; each spanning tree instance is identified by an instance ID that ranges from 0 to 15. Instance 0 is mandatory and is always present. Instances 1 through 15 are option

MST Configuration Parameters

MST configuration includes these three parts:

- Name—A 32-character string (null padded) identifying the MST region.
- Revision number—An unsigned 16-bit number that identifies the revision of the current MST configuration.

Note You must set the revision number when required as part of the MST configuration. The revision number is not incremented automatically each time you commit the MST configuration.

- MST configuration table—An array of 4096 bytes. Each byte, interpreted as an unsigned integer, corresponds to a VLAN. The value is the instance number to which the VLAN is mapped. The first byte that corresponds to VLAN 0 and the 4096th byte that corresponds to VLAN 4095 are unused and always set to zero.

You must configure each byte manually. You can use SNMP or the CLI to perform the configuration.

MST BPDUs contain the MST configuration ID and the checksum. An MST bridge accepts an MST BPDU only if the MST BPDU configuration ID and the checksum match its own MST region configuration ID and checksum. If one value is different, the MST BPDU is considered to be an SST BPDU.

MST Regions

These sections describe MST regions:

- MST Region Overview, page 15-19
- Boundary Ports, page 15-19
- IST Master, page 15-19
- Edge Ports, page 15-20
- Link Type, page 15-20

MST Region Overview

Interconnected bridges that have the same MST configuration are referred to as an MST region. There is no limit on the number of MST regions in the network.

To form an MST region, bridges can be either of the following:

- An MST bridge that is the only member of the MST region.
- An MST bridge interconnected by a LAN. A LAN's designated bridge has the same MST configuration as an MST bridge. All the bridges on the LAN can process MST BPDUs.

If you connect two MST regions with different MST configurations, the MST regions do the following:

- Load balance across redundant paths in the network. If two MST regions are redundantly connected, all traffic flows on a single connection with the MST regions in a network.
- Provide an RSTP handshake to enable rapid connectivity between regions. However, the handshaking is not as fast as between two bridges. To prevent loops, all the bridges inside the region must agree upon the connections to other regions. This situation introduces a delay. We do not recommend partitioning the network into a large number of regions.

Boundary Ports

A boundary port is a port that connects to a LAN, the designated bridge, of which is either an SST bridge, or a bridge with a different MST configuration. A designated port knows that it is on the boundary if it detects an STP bridge or receives an agreement message from an RST or MST bridge with a different configuration.

At the boundary, the role of MST ports do not matter; their state is forced to be the same as the IST port state. If the boundary flag is set for the port, the MSTP port-role selection process assigns a port role to the boundary and assigns the same state as the state of the IST port. The IST port at the boundary can take up any port role except a backup port role.

IST Master

The IST master of an MST region is the bridge with the lowest bridge identifier and the least path cost to the CST root. If an MST bridge is the root bridge for CST, then it is the IST master of that MST region. If the CST root is outside the MST region, then one of the MST bridges at the boundary is selected as the IST master. Other bridges on the boundary that belong to the same region eventually block the boundary ports that lead to the root.

If two or more bridges at the boundary of a region have an identical path to the root, you can set a slightly lower bridge priority to make a specific bridge the IST master.

The root path cost and message age inside a region stay constant, but the IST path cost is incremented and the IST remaining hops are decremented at each hop. To display the information about the IST master, path cost, and remaining hops for the bridge, enter the **show spanning-tree mst** command.

Edge Ports

An edge port is a port that is a port that is connected to a nonbridging device (for example, a host or a router). A port that connects to a hub is also an edge port if the hub or any LAN that is connected by it does not have a bridge. An edge port can start forwarding as soon as the link is up.

MST requires that you configure all ports for each host or router. To establish rapid connectivity after a failure, you need to block the nonedge designated ports of an intermediate bridge. If the port connects to another bridge that can send back an agreement, then the port starts forwarding immediately. Otherwise, the port needs twice the forward delay time to start forwarding again. You must explicitly configure the ports that are connected to the hosts and routers as edge ports while using MST.

To prevent a misconfiguration, the PortFast operation is turned off if the port receives a BPDU. To display the configured and operational status of PortFast, enter the **show spanning-tree mst** *interfac* command.

Link Type

Rapid connectivity is established only on point-to-point links. You must configure ports explicitly to a host or router. However, cabling in most networks meets this requirement, and you can avoid explicit configuration by treating all full-duplex links as point-to-point links by entering the **spanning-tree linktype** command.

Message Age and Hop Count

IST and MST instances do not use the message age and maximum age timer settings in the BPDU. IST and MST use a separate hop-count process that is very similar to the IP TTL process. You can configure each MST bridge with a maximum hop count. The root bridge of the instance sends a BPDU (or M-record) with the remaining hop count that is equal to the maximum hop count. When a bridge receives a BPDU (or M-record), it decrements the received remaining hop count by one. The bridge discards the BPDU (M-record) and ages out the information held for the port if the count reaches zero after decrementing. The nonroot bridges propagate the decremented count as the remaining hop count in th BPDUs (M-records) they generate.

The message age and maximum age timer settings in the RST portion of the BPDU remain the same throughout the region, and the same values are propagated by the region's designated ports at the boundary.

Default STP Configuration

Table 15-5 shows the default STP configuration.

Table 15-5 STP Default Configuration

Feature	Default Value
Enable state	STP enabled for all VLANs
Bridge priority	32768
STP port priority (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)	128
STP port cost (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)	• 10-Gigabit Ethernet: 2 • Gigabit Ethernet: 4 • Fast Ethernet: 19 • Ethernet: 100
STP VLAN port priority (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports)	128
STP VLAN port cost (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports)	• 10-Gigabit Ethernet: 2 • Gigabit Ethernet: 4 • Fast Ethernet: 19 • Ethernet: 100
Hello time	2 seconds
Forward delay time	15 seconds
Maximum aging time	20 seconds
Mode	PVST

STP and MST Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when configuring MST:

- Do not disable spanning tree on any VLAN in any of the PVST bridges.
- Do not use PVST bridges as the root of CST.
- Ensure that all PVST spanning tree root bridges have lower (numerically higher) priority than the CST root bridge.

- Ensure that trunks carry all of the VLANs mapped to an instance or do not carry any VLANs at all for this instance.
- Do not connect switches with access links because access links may partition a VLAN.
- Any MST configuration involving a large number of either existing or new logical VLAN ports should be completed during a maintenance window because the complete MST database gets reinitialized for any incremental change (such as adding new VLANs to instances or moving VLANs across instances).

Configuring STP

These sections describe how to configure STP on VLANs:

- Enabling STP, page 15-23
- Enabling the Extended System ID, page 15-24
- Configuring the Root Bridge, page 15-25
- Configuring a Secondary Root Bridge, page 15-26
- Configuring STP Port Priority, page 15-27
- Configuring STP Port Cost, page 15-29
- Configuring the Bridge Priority of a VLAN, page 15-30
- Configuring the Hello Time, page 15-32
- Configuring the Forward-Delay Time for a VLAN, page 15-32
- Configuring the Maximum Aging Time for a VLAN, page 15-33
- Enabling Rapid-PVST, page 15-33

Note

- The STP commands described in this chapter can be configured on any LAN port, but they are in effect only on LAN ports configured with the **switchport** keyword.
- With Release 12.1(11b)E and later releases, when you are in configuration mode you can enter EXEC mode-level commands by entering the **do** keyword before the EXEC mode-level command.

Caution

We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree serves as a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

Enabling STP

Note STP is enabled by default on VLAN 1 and on all newly created VLANs.

You can enable STP on a per-VLAN basis. The Catalyst 6500 series switch maintains a separate instance of STP for each VLAN (except on VLANs on which you disable STP).

To enable STP on a per-VLAN basis, perform this task:

	Command	Purpose
Step 1	`Router(config)# spanning-tree vlan vlan_ID`	Enables STP on a per-VLAN basis. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 15-5 on page 15-21).
	`Router(config)# default spanning-tree vlan vlan_ID`	Reverts all STP parameters to default values for the specified VLAN.
	`Router(config)# no spanning-tree vlan vlan_ID`	Disables STP on the specified VLAN; see the following Cautions for information regarding this command.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show spanning-tree vlan vlan_ID`	Verifies that STP is enabled.

Caution Do not disable spanning tree on a VLAN unless all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the VLAN. This action can have unexpected results because switches and bridges with spanning tree enabled will have incomplete information regarding the physical topology of the network.

Caution We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree serves as a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

This example shows how to enable STP on VLAN 200:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200
Router(config)# end
Router#
```

Note Because STP is enabled by default, entering a **show running** command to view the resulting configuration does not display the command you entered to enable STP.

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200

VLAN0200
  Spanning tree enabled protocol ieee
  Root ID     Priority     32768
              Address      00d0.00b8.14c8
              This bridge is the root
              Hello Time    2 sec   Max Age 20 sec   Forward Delay 15 sec

  Bridge ID   Priority     32768
              Address      00d0.00b8.14c8
              Hello Time    2 sec   Max Age 20 sec   Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Desg FWD 200000    128.196  P2p
Fa4/5            Back BLK 200000    128.197  P2p

Router#
```

Note You must have at least one interface that is active in VLAN 200 to create a VLAN 200 spanning tree. In this example, two interfaces are active in VLAN 200.

Enabling the Extended System ID

Note The extended system ID is enabled permanently on chassis that support 64 MAC addresses.

You can enable the extended system ID on chassis that support 1024 MAC addresses (see the "Understanding the Bridge ID" section on page 15-3).

To enable the extended system ID, perform this task:

	Command	Purpose
Step 1	`Router(config)# spanning-tree extend system-id`	Enables the extended system ID.
	`Router(config)# no spanning-tree extend system-id`	Disables the extended system ID. **Note** You cannot disable the extended system ID on chassis that support 64 MAC addresses or when you have configured extended range VLANs (see "STP Default Configuration" section on page 15-21).
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show spanning-tree vlan vlan_ID`	Verifies the configuration.

Note When you enable or disable the extended system ID, the bridge IDs of all active STP instances are updated, which might change the spanning tree topology.

This example shows how to enable the extended system ID:

```
Router# configure terminal
Router(config)# spanning-tree extend system-id
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree summary | include Extended
Extended system ID is enabled.
```

Configuring the Root Bridge

Catalyst 6500 series switches maintain a separate instance of STP for each active VLAN. A bridge ID, consisting of the bridge priority and the bridge MAC address, is associated with each instance. For each VLAN, the network device with the lowest bridge ID becomes the root bridge for that VLAN.

To configure a VLAN instance to become the root bridge, enter the **spanning-tree vlan** *vlan_ID* **root** command to modify the bridge priority from the default value (32768) to a significantly lower value.

When you enter the **spanning-tree vlan** *vlan_ID* **root** command, the switch checks the bridge priority of the current root bridges for each VLAN. When the extended system ID is disabled, the switch sets the bridge priority for the specified VLANs to 8192 if this value will cause the switch to become the root for the specified VLANs. When the extended system ID is enabled, the switch sets the bridge priority for the specified VLANs to 24576 if this value will cause the switch to become the root for the specified VLANs.

If the extended system ID is disabled and if any root bridge for the specified VLANs has a bridge priority lower than 8192, the switch sets the bridge priority for the specified VLANs to 1 less than the lowest bridge priority.

If the extended system ID is enabled and if any root bridge for the specified VLANs has a bridge priority lower than 24576, the switch sets the bridge priority for the specified VLANs to 4096 less than the lowest bridge priority. (4096 is the value of the least significant bit of a 4-bit bridge priority value; see Table 15-2 on page 15-3.)

Note The **spanning-tree vlan** *vlan_ID* **root** command fails if the value required to be the root bridge is less than 1.

The **spanning-tree vlan** *vlan_ID* **root** command can cause the following effects:

- If the extended system ID is disabled, and if all network devices in VLAN 100 have the default priority of 32768, entering the **spanning-tree vlan 100 root primary** command on the switch sets the bridge priority for VLAN 100 to 8192, which causes the switch to become the root bridge for VLAN 100.
- If the extended system ID is enabled, and if all network devices in VLAN 20 have the default priority of 32768, entering the **spanning-tree vlan 20 root primary** command on the switch sets the bridge priority to 24576, which causes the switch to become the root bridge for VLAN 20.

Caution The root bridge for each instance of STP should be a backbone or distribution switch. Do not configure an access switch as the STP primary root.

Use the **diameter** keyword to specify the Layer 2 network diameter (that is, the maximum number of bridge hops between any two end stations in the Layer 2 network). When you specify the network diameter, the Catalyst 6500 series switch automatically selects an optimal hello time, forward delay time, and maximum age time for a network of that diameter, which can significantly reduce the STP convergence time. You can use the **hello** keyword to override the automatically calculated hello time.

Note To preserve a stable STP topology, we recommend that you avoid configuring the hello time, forward delay time, and maximum age time manually after configuring the Catalyst 6500 series switch as the root bridge.

To configure a Catalyst 6500 series switch as the root bridge, perform this task:

	Command	Purpose
Step 1	Router(config)# **spanning-tree vlan** *vlan_ID* **root primary** [**diameter** *hops* [**hello-time** *seconds*]]	Configures a Catalyst 6500 series switch as the root bridge. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 15-5 on page 15-21).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **root**	Clears the root bridge configuration.
Step 2	Router(config)# **end**	Exits configuration mode.

This example shows how to configure the Catalyst 6500 series switch as the root bridge for VLAN 10, with a network diameter of 4:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# end
Router#
```

Configuring a Secondary Root Bridge

When you configure a Catalyst 6500 series switch as the secondary root, the STP bridge priority is modified from the default value (32768) so that the switch is likely to become the root bridge for the specified VLANs if the primary root bridge fails (assuming the other network devices in the network use the default bridge priority of 32768).

If the extended system ID is enabled, STP sets the bridge priority to 28672. If the extended system ID is disabled, STP sets the bridge priority to 16384.

You can run this command on more than one Catalyst 6500 series switch to configure multiple backup root bridges. Use the same network diameter and hello time values as you used when configuring the primary root bridge.

To configure a Catalyst 6500 series switch as the secondary root bridge, perform this task:

	Command	Purpose
Step 1	Router(config)# [no] **spanning-tree vlan** *vlan_ID* **root secondary** [**diameter** *hops* [**hello-time** *seconds*]]	Configures a Catalyst 6500 series switch as the secondary root bridge. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 9-1 on page 9-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **root**	Clears the root bridge configuring.
Step 2	Router(config)# **end**	Exits configuration mode.

This example shows how to configure the Catalyst 6500 series switch as the secondary root bridge for VLAN 10, with a network diameter of 4:

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root secondary diameter 4
Router(config)# end
Router#
```

Configuring STP Port Priority

If a loop occurs, STP considers port priority when selecting a LAN port to put into the forwarding state. You can assign higher priority values to LAN ports that you want STP to select first and lower priority values to LAN ports that you want STP to select last. If all LAN ports have the same priority value, STP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports. The possible priority range is 0 through 240 (default 128), configurable in increments of 16.

Cisco IOS uses the port priority value when the LAN port is configured as an access port and uses VLAN port priority values when the LAN port is configured as a trunk port.

To configure the STP port priority of a Layer 2 LAN interface, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface** {{*type*[1] *slot/port*} | {**port-channel** *port_channel_number*}}	Selects an interface to configure.
Step 2	Router(config-if)# **spanning-tree port-priority** *port_priority*	Configures the port priority for the LAN interface. The *port_priority* value can be from 1 to 252 in increments of 4.
	Router(config-if)# **no spanning-tree port-priority**	Reverts to the default port priority value.
Step 3	Router(config-if)# **spanning-tree vlan** *vlan_ID* **port-priority** *port_priority*	Configures the VLAN port priority for the LAN interface. The *port_priority* value can be from 1 to 252 in increments of 4. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 9-1 on page 9-2).
	Router(config-if)# [no] **spanning-tree vlan** *vlan_ID* **port-priority**	Reverts to the default VLAN port priority value.
Step 4	Router(config-if)# **end**	Exits configuration mode.

	Command	Purpose

Step 5	`Router# show spanning-tree interface {type[1] slot/port} | {port-channel port_channel_number}`
	`Router# show spanning-tree vlan vlan_ID`
		Verifies the configuration.

[1] *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure the STP port priority of Fast Ethernet port 4/4:

```
Router# configure terminal
Router(config)# interface fastethernet 4/4
Router(config-if)# spanning-tree port-priority 160
Router(config-if)# end
Router#
```

This example shows how to verify the configuration of Fast Ethernet port 4/4:

```
Router# show spanning-tree interface fastethernet 4/4
Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Back BLK 200000    160.196  P2p
VLAN0006         Back BLK 200000    160.196  P2p
...
VLAN0198         Back BLK 200000    160.196  P2p
VLAN0199         Back BLK 200000    160.196  P2p
VLAN0200         Back BLK 200000    160.196  P2p
Router#
```

Fastethernet 4/4 is a trunk. Several VLANs are configured and active as shown in the example. The port priority configuration applies to all VLANs on this interface.

Note The **show spanning-tree interface** command only displays information if the port is connected and operating. If this condition is not met, enter a **show running-config interface** command to verify the configuration.

This example shows how to configure the VLAN port priority of Fast Ethernet port 4/4:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree vlan 200 port-priority 64
Router(config-if)# ^Z
Router#
```

The configuration entered in the example only applies to VLAN 200. All VLANs other than 200 still have a port priority of 160.

This example shows how to verify the configuration:

```
Router# show spanning-tree interface fastethernet 4/4
Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Back BLK 200000    160.196  P2p
VLAN0006         Back BLK 200000    160.196  P2p
...
VLAN0199         Back BLK 200000    160.196  P2p
VLAN0200         Desg FWD 200000     64.196  P2p

Router#
```

You also can display spanning tree information for VLAN 200 using the following command:

```
Router# show spanning-tree vlan 200 interface fastEthernet 4/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Desg LRN 200000     64.196  P2p
```

Configuring STP Port Cost

The STP port path cost default value is determined from the media speed of a LAN interface. If a loop occurs, STP considers port cost when selecting a LAN interface to put into the forwarding state. You can assign lower cost values to LAN interfaces that you want STP to select first and higher cost values to LAN interfaces that you want STP to select last. If all LAN interfaces have the same cost value, STP puts the LAN interface with the lowest LAN interface number in the forwarding state and blocks other LAN interfaces. The possible cost range is 0 through 200000000 (the default is media specific).

STP uses the port cost value when the LAN interface is configured as an access port and uses VLAN port cost values when the LAN interface is configured as a trunk port.

To configure the STP port cost of a Layer 2 LAN interface, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface {{type[1] slot/port} | {port-channel port_channel_number}}`	Selects an interface to configure.
Step 2	`Router(config-if)# spanning-tree cost port_cost`	Configures the port cost for the LAN interface. The *port_cost* value can be from 1 to 200000000 (1 to 65535 in Release 12.1(2)E and earlier releases).
	`Router(config-if)# no spanning-tree cost`	Reverts to the default port cost.
Step 3	`Router(config-if)# [no] spanning-tree vlan vlan_ID cost port_cost`	Configures the VLAN port cost for the LAN interface. The *port_cost* value can be from 1 to 200000000. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 9-1 on page 9-2).
Step 4	`Router(config-if)# no spanning-tree vlan vlan_ID cost`	Reverts to the default VLAN port cost.
Step 5	`Router(config-if)# end`	Exits configuration mode.

Step 6	`Router# show spanning-tree interface {type[1] slot/port} | {port-channel port_channel_number}`
	`show spanning-tree vlan vlan_ID`
		Verifies the configuration.

[1] *type* = **ethernet, fastethernet, gigabitethernet,** or **tengigabitethernet**

This example shows how to change the STP port cost of Fast Ethernet port 4/4:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree cost 1000
Router(config-if)# ^Z
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree interface fastEthernet 4/4
Vlan             Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Back BLK 1000      160.196  P2p
```

```
VLAN0006         Back BLK 1000      160.196  P2p
VLAN0007         Back BLK 1000      160.196  P2p
VLAN0008         Back BLK 1000      160.196  P2p
VLAN0009         Back BLK 1000      160.196  P2p
VLAN0010         Back BLK 1000      160.196  P2p
Router#
```

This example shows how to configure the port priority at an individual port VLAN cost for VLAN 200:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree vlan 200 cost 2000
Router(config-if)# ^Z
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 interface fastEthernet 4/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Desg FWD 2000       64.196  P2p
```

Note In the following output other VLANs (VLAN 1 for example) have not been affected by this configuration.

```
Router# show spanning-tree vlan 1 interface fastEthernet 4/4
Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Router#
```

Note The **show spanning-tree** command only displays information for ports that are in link-up operative state and are appropriately configured for DTP. If these conditions are not met, you can enter a **show running-config** command to confirm the configuration.

Configuring the Bridge Priority of a VLAN

Note Be careful when using this command. For most situations, we recommend that you enter the **spanning-tree vlan** *vlan_ID* **root primary** and the **spanning-tree vlan** *vlan_ID* **root secondary** commands to modify the bridge priority.

To configure the STP bridge priority of a VLAN when the extended system ID is disabled, perform this task:

	Command	Purpose
Step 1	Router(config)# **spanning-tree vlan** *vlan_ID* **priority** *bridge_priority*	Configures the bridge priority of a VLAN when the extended system ID is disabled. The *bridge_priority* value can be from 1 to 65535. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 9-1 on page 9-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **priority**	Reverts to the default bridge priority value.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show spanning-tree vlan** *vlan_ID* **bridge** [**detail**]	Verifies the configuration.

To configure the STP bridge priority of a VLAN when the extended system ID is enabled, perform this task:

	Command	Purpose
Step 1	Router(config)# [**no**] **spanning-tree vlan** *vlan_ID* **priority** {**0** | **4096** | **8192** | **12288** | **16384** | **20480** | **24576** | **28672** | **32768** | **36864** | **40960** | **45056** | **49152** | **53248** | **57344** | **61440**}	Configures the bridge priority of a VLAN when the extended system ID is enabled. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 9-1 on page 9-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **priority**	Reverts to the default bridge priority value.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show spanning-tree vlan** *vlan_ID* **bridge** [**detail**]	Verifies the configuration.

This example shows how to configure the bridge priority of VLAN 200 to 33792 when the extended system ID is disabled:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 priority 33792
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
                                      Hello Max  Fwd
Vlan                    Bridge ID     Time  Age  Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200           33792 0050.3e8d.64c8    2   20    15  ieee
Router#
```

Configuring the Hello Time

Note Be careful when using this command. For most situations, we recommend that you use the **spanning-tree vlan** *vlan_ID* **root primary** and **spanning-tree vlan** *vlan_ID* **root secondary** commands to modify the hello time.

To configure the STP hello time of a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# **spanning-tree vlan** *vlan_ID* **hello-time** *hello_time*	Configures the hello time of a VLAN. The *hello_time* value can be from 1 to 10 seconds. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 9-1 on page 9-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **hello-time**	Reverts to the default hello time.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show spanning-tree vlan** *vlan_ID* **bridge** [**detail**]	Verifies the configuration.

This example shows how to configure the hello time for VLAN 200 to 7 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 hello-time 7
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
                                       Hello  Max  Fwd
Vlan                       Bridge ID   Time   Age  Delay  Protocol
---------------- --------------------  ----  ----  -----  --------
VLAN200          49152 0050.3e8d.64c8     7    20     15  ieee
Router#
```

Configuring the Forward-Delay Time for a VLAN

To configure the STP forward delay time for a VLAN, perform this task:

	Command	Purpose
Step 1	Router(config)# **spanning-tree vlan** *vlan_ID* **forward-time** *forward_time*	Configures the forward time of a VLAN. The *forward_time* value can be from 4 to 30 seconds. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 9-1 on page 9-2).
	Router(config)# **no spanning-tree vlan** *vlan_ID* **forward-time**	Reverts to the default forward time.
Step 2	Router(config)# **end**	Exits configuration mode.
Step 3	Router# **show spanning-tree vlan** *vlan_ID* **bridge** [**detail**]	Verifies the configuration.

This example shows how to configure the forward delay time for VLAN 200 to 21 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 forward-time 21
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
                                      Hello Max  Fwd
Vlan                       Bridge ID  Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          49152 0050.3e8d.64c8    2   20    21  ieee
Router#
```

Configuring the Maximum Aging Time for a VLAN

To configure the STP maximum aging time for a VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# spanning-tree vlan vlan_ID max-age max_age`	Configures the maximum aging time of a VLAN. The *max_age* value can be from 6 to 40 seconds. The *vlan_ID* value can be 1 through 4094, except reserved VLANs (see Table 9-1 on page 9-2).
	`Router(config)# no spanning-tree vlan vlan_ID max-age`	Reverts to the default maximum aging time.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show spanning-tree vlan vlan_ID bridge [detail]`	Verifies the configuration.

This example shows how to configure the maximum aging time for VLAN 200 to 36 seconds:

```
Router# configure terminal
Router(config)# spanning-tree vlan 200 max-age 36
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree vlan 200 bridge
                                      Hello Max  Fwd
Vlan                       Bridge ID  Time  Age Delay  Protocol
---------------- -------------------- ---- ---- -----  --------
VLAN200          49152 0050.3e8d.64c8    2   36    15  ieee
Router#
```

Enabling Rapid-PVST

Rapid-PVST uses the existing PVST+ framework for configuration and interaction with other features. It also supports some of the PVST+ extensions.

To enable Rapid-PVST mode on the switch, enter the **spanning-tree mode rapid-pvst** command in privileged mode. To configure the switch in Rapid-PVST mode, see the "Configuring STP" section on page 15-22.

Specifying the Link Type

Rapid connectivity is established only on point-to-point links. Spanning tree views a point-to-point link as a segment connecting only two switches running the spanning tree algorithm. Because the switch assumes that all full-duplex links are point-to-point links and that half-duplex links are shared links, you can avoid explicitly configuring the link type. To configure a specific link type, enter the **spanning-tree linktype** command.

Restarting Protocol Migration

A switch running both MSTP and RSTP supports a built-in protocol migration process that enables the switch to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, or an MST BPDU (version 3) associated with a different region, or an RST BPDU (version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. A switch also might continue to assign a boundary role to port when the switch to which it is connected has joined the region.

To restart the protocol migration process (force the renegotiation with neighboring switches) on the entire switch, you can use the **clear spanning-tree detected-protocols** privileged EXEC command. To restart the protocol migration process on a specific interface, enter the **clear spanning-tree detected-protocols interface** *interface-id* privileged EXEC command.

Configuring IEEE 802.1s MST

Release 12.1(13)E and later releases support MST. These sections describe how to configure MST:

- Enabling MST, page 15-34
- Displaying MST Configurations, page 15-36
- Configuring MST Instance Parameters, page 15-39
- Configuring MST Instance Port Parameters, page 15-40
- Restarting Protocol Migration, page 15-40

Enabling MST

To enable and configure MST on the switch, perform these tasks in privileged mode:

	Command	Purpose
Step 1	Router# **show spanning-tree mst configuration**	Displays the current MST configuration.
Step 2	Router(config)# **spanning-tree mode mst**	Configures MST mode.
Step 3	Router(config)# **spanning-tree mst configuration**	Configures the MST region by entering the MST configuration submode.
	Router(config)# **no spanning-tree mst configuration**	Clears the MST configuration.

	Command	Purpose
Step 4	`Router(config-mst)# show current`	Displays the current MST configuration from within the MST configuration submode
Step 5	`Router(config-mst)# name name revision revision_number instance instance_number vlan vlan_range`	Enters the MST configuration.
Step 6	`Router(config-mst)# no instance instance_number`	(Optional) Unmaps all VLANs that were mapped to an instance.
Step 7	`Router(config-mst)# no instance instance_number vlan vlan_number`	(Optional) Unmaps a VLAN from an instance.
Step 8	`Router(config-mst)# end`	Applies the configuration and exit configuration mode.
Step 9	`Router# show spanning-tree mst config`	Shows the MST configuration from the global configuration mode.

These examples show how to enable MST:

```
Router# show spanning-tree mst configuration
% Switch is not in mst mode
Name      []
Revision  0
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
-------------------------------------------------------------------------------

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# spanning-tree mode mst

Router(config)# spanning-tree mst configuration

Router(config-mst)# show current
Current MST configuration
Name      []
Revision  0
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
-------------------------------------------------------------------------------

Router(config-mst)# name cisco
Router(config-mst)# revision 2
Router(config-mst)# instance 1 vlan 1
Router(config-mst)# instance 2 vlan 1-1000
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1001-4094
2         1-1000
-------------------------------------------------------------------------------

Router(config-mst)# no instance 2
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
-------------------------------------------------------------------------------
```

```
Router(config-mst)# instance 1 vlan 2000-3000
Router(config-mst)# show pending
Pending MST configuration
Name      [cisco]
Revision  2
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-1999,2500,3001-4094
1         2000-2499,2501-3000
-------------------------------------------------------------------------------
Router(config)# exit
Router(config)# no spanning-tree mst configuration
Router(config)# do show spanning-tree mst configuration
Name      []
Revision  0
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         1-4094
-------------------------------------------------------------------------------
```

Displaying MST Configurations

To display MST configurations, perform these tasks in MST mode:

	Command	Purpose
Step 1	Router# **show spanning-tree mst configuration**	Displays the active configuration
Step 2	Router# **show spanning-tree mst** [**detail**]	Displays information about the MST instances currently running.
Step 3	Router# **show spanning-tree mst** *instance-id* [*detail*]	Displays information about a specific MST instance
Step 4	Router# **show spanning-tree mst interface** *interface name* [**detail**]	Displays information for a given port.
Step 5	Router# **show spanning-tree mst** *number* **interface** *interface name* [**detail**]	Displays MST information for a given port and a given instance
Step 6	Router# **show spanning-tree mst** [*x*] [*interface Y*] *detail*	Displays detailed MST information.
Step 7	Router# **show spanning-tree vlan** *vlan_ID*	Displays VLAN information in MST mode.

These examples show how to display spanning tree VLAN configurations in MST mode:

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 1-10
Router(config-mst)# name cisco
Router(config-mst)# revision 1
Router(config-mst)# ^Z

Router# show spanning-tree mst configuration
Name      [cisco]
Revision  1
Instance  Vlans mapped
--------  ---------------------------------------------------------------------
0         11-4094
1         1-10
-------------------------------------------------------------------------------
```

```
Router# show spanning-tree mst

###### MST00         vlans mapped:  11-4094
Bridge       address 00d0.00b8.1400  priority  32768 (32768 sysid 0)
Root         address 00d0.004a.3c1c  priority  32768 (32768 sysid 0)
             port    Fa4/48          path cost 203100
IST master   this switch
Operational  hello time 2, forward delay 15, max age 20, max hops 20
Configured   hello time 2, forward delay 15, max age 20, max hops 20

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Root FWD 200000    128.240  P2p Bound(STP)

###### MST01         vlans mapped:  1-10
Bridge       address 00d0.00b8.1400  priority  32769 (32768 sysid 1)
Root         this switch for MST01

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Boun FWD 200000    128.240  P2p Bound(STP)


Router# show spanning-tree mst 1

###### MST01         vlans mapped:  1-10
Bridge       address 00d0.00b8.1400  priority  32769 (32768 sysid 1)
Root         this switch for MST01

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Boun FWD 200000    128.240  P2p Bound(STP)

Router# show spanning-tree mst interface fastEthernet 4/4

FastEthernet4/4 of MST00 is backup blocking
Edge port:no             (default)        port guard :none        (default)
Link type:point-to-point (auto)           bpdu filter:disable     (default)
Boundary :internal                        bpdu guard :disable     (default)
Bpdus sent 2, received 368

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- -------------------------------
0        Back BLK 1000      160.196  11-4094
1        Back BLK 1000      160.196  1-10

Router# show spanning-tree mst 1 interface fastEthernet 4/4

FastEthernet4/4 of MST01 is backup blocking
Edge port:no             (default)        port guard :none        (default)
Link type:point-to-point (auto)           bpdu filter:disable     (default)
Boundary :internal                        bpdu guard :disable     (default)
Bpdus (MRecords) sent 2, received 364

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- -------------------------------
1        Back BLK 1000      160.196  1-10
```

```
Router# show spanning-tree mst 1 detail

###### MST01        vlans mapped:  1-10
Bridge      address 00d0.00b8.1400  priority  32769 (32768 sysid 1)
Root        this switch for MST01

FastEthernet4/4 of MST01 is backup blocking
Port info             port id         160.196  priority    160  cost        1000
Designated root       address 00d0.00b8.1400  priority  32769  cost           0
Designated bridge     address 00d0.00b8.1400  priority  32769  port id  128.197
Timers:message expires in 5 sec, forward delay 0, forward transitions 0
Bpdus (MRecords) sent 123, received 1188

FastEthernet4/5 of MST01 is designated forwarding
Port info             port id         128.197  priority    128  cost      200000
Designated root       address 00d0.00b8.1400  priority  32769  cost           0
Designated bridge     address 00d0.00b8.1400  priority  32769  port id  128.197
Timers:message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 1188, received 123

FastEthernet4/48 of MST01 is boundary forwarding
Port info             port id         128.240  priority    128  cost      200000
Designated root       address 00d0.00b8.1400  priority  32769  cost           0
Designated bridge     address 00d0.00b8.1400  priority  32769  port id  128.240
Timers:message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus (MRecords) sent 78, received 0

Router# show spanning-tree vlan 10

MST01
  Spanning tree enabled protocol mstp
  Root ID    Priority    32769
             Address     00d0.00b8.1400
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     00d0.00b8.1400
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p

Router# show spanning-tree summary
Root bridge for:MST01
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
UplinkFast           is disabled
BackboneFast         is disabled
Pathcost method used is long

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
MST00                      1         0         0        2          3
MST01                      1         0         0        2          3
---------------------- -------- --------- -------- ---------- ----------
2 msts                     2         0         0        4          6
Router#
```

Configuring MST Instance Parameters

To configure MST instance parameters, perform these tasks:

	Command	Purpose
Step 1	Router(config)# **spanning-tree mst** *X* **priority** *Y*	Configures the priority for an MST instance
Step 2	Router(config)# **spanning-tree mst** *X* **root** [**primary** | **secondary**]	Configures the bridge as root for an MST instance.
Step 3	Router# **show spanning-tree mst**	Verifies the configuration.

This example shows how to configure MST instance parameters:

```
Router(config)# spanning-tree mst 1 priority ?
  <0-61440>  bridge priority in increments of 4096

Router(config)# spanning-tree mst 1 priority 1
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0     4096  8192  12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440

Router(config)# spanning-tree mst 1 priority 49152
Router(config)#

Router(config)# spanning-tree mst 0 root primary
 mst 0 bridge priority set to 24576
 mst bridge max aging time unchanged at 20
 mst bridge hello time unchanged at 2
 mst bridge forward delay unchanged at 15
Router(config)# ^Z
Router#

Router# show spanning-tree mst

###### MST00         vlans mapped:  11-4094
Bridge       address 00d0.00b8.1400  priority  24576 (24576 sysid 0)
Root         this switch for CST and IST
Configured   hello time 2, forward delay 15, max age 20, max hops 20

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Desg FWD 200000    128.240  P2p Bound(STP)

###### MST01         vlans mapped:  1-10
Bridge       address 00d0.00b8.1400  priority  49153 (49152 sysid 1)
Root         this switch for MST01

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- --------------------------------
Fa4/4            Back BLK 1000      160.196  P2p
Fa4/5            Desg FWD 200000    128.197  P2p
Fa4/48           Boun FWD 200000    128.240  P2p Bound(STP)

Router#
```

Configuring MST Instance Port Parameters

To configure MST instance port parameters, perform these tasks:

	Command	Purpose
Step 1	`Router(config-if)# spanning-tree mst x cost y`	Configures the MST instance port cost.
Step 2	`Router(config-if)# spanning-tree mst x port-priority y`	Configures the MST instance port priority.
Step 3	`Router# show spanning-tree mst x interface y`	Verifies the configuration.

This example shows how to configure MST instance port parameters:

```
Router(config)# interface fastEthernet 4/4
Router(config-if)# spanning-tree mst 1 ?
  cost           Change the interface spanning tree path cost for an instance
  port-priority  Change the spanning tree port priority for an instance

Router(config-if)# spanning-tree mst 1 cost 1234567
Router(config-if)# spanning-tree mst 1 port-priority 240
Router(config-if)# ^Z

Router# show spanning-tree mst 1 interface fastEthernet 4/4

FastEthernet4/4 of MST01 is backup blocking
Edge port:no            (default)        port guard :none        (default)
Link type:point-to-point (auto)          bpdu filter:disable     (default)
Boundary :internal                       bpdu guard :disable     (default)
Bpdus (MRecords) sent 125, received 1782

Instance Role Sts Cost      Prio.Nbr Vlans mapped
-------- ---- --- --------- -------- -------------------------------
1        Back BLK 1234567   240.196  1-10

Router#
```

Restarting Protocol Migration

A switch running both MSTP and RSTP supports a built-in protocol migration mechanism that enables the switch to interoperate with legacy 802.1D switches. If this switch receives a legacy 802.1D configuration BPDU (a BPDU with the protocol version set to 0), it sends only 802.1D BPDUs on that port. An MSTP switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (version 3) associated with a different region, or an RST BPDU (version 2).

However, the switch does not automatically revert to the MSTP mode if it no longer receives 802.1D BPDUs because it cannot determine whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. A switch also might continue to assign a boundary role to a port when the switch to which it is connected has joined the region.

To restart the protocol migration process (force the renegotiation with neighboring switches) on the entire switch, you can use the **clear spanning-tree detected-protocols** privileged EXEC command. Use the **clear spanning-tree detected-protocols interface** *interface-id* privileged EXEC command to restart the protocol migration process on a specific interface.

This example shows how to restart protocol migration:

```
Router# clear spanning-tree detected-protocols interface fastEthernet 4/4
Router#
```

Apêndice FF

CISCO SYSTEMS

Data Sheet

Cisco Catalyst 6500 **Supervisor** Engines 1A and 2

As Cisco's premier modular multilayer switch, the Catalyst® 6500 Series delivers secure, converged services from the wiring closet to the core, to the data center to the WAN edge.

The supervisor engines for the Catalyst 6500 Series deliver the latest advanced switching technology with proven Cisco software to power a new generation of scalable and intelligent multilayer switching solutions for both enterprise and service provider environments. Designed to integrate data, voice, and video into a single platform for fully integrated IP communications, the Catalyst 6500 Series supervisor engines enable intelligent, resilient, scalable, and secure high performance multilayer switching solutions.

The widely deployed Supervisor Engine 1A and Supervisor Engine 2 are used in wiring closets, distribution/core, data center and WAN edge configurations enabling the seamless integration of advanced services such as security, voice and content into a converged network that reduces the total cost of ownership. And the new Supervisor Engine 720 is ideally suited for high performance core, data center and metro Ethernet deployments with its scalable performance of up to 400 million packets per second using a 720Gbps switch fabric.

By sharing a common set of interfaces, operating system and management tools, the Catalyst 6500 Series supervisors provide operational consistency—enabling common sparing and minimizing training requirements; all modules feature predictable performance and a broad range of capabilities. Supervisor Engine 1A and Supervisor Engine 2 highlights include:

- *Feature-rich and wire-rate intelligent network services*—Support and complement comprehensive security and granular Quality of Service mechanisms, including identity-based networking capabilities based on IEEE 802.1x extensions and simplified configuration using two AutoQoS commands
- *End-to-end flexible deployments*—Position anywhere in the network from the wiring closet to the distribution/core, and from the data center to the WAN edge and the MAN
- *Scaleable and predictable performance*—Feature a flexible switch fabric and forwarding architecture delivering throughput from 15Mpps/32Gbps (Classic interface modules), to 30Mpps/256Gbps (CEF256 interface modules), to 210Mpps/256Gbps (dCEF256 interface modules) for network cores supporting multi-gigabit trunks
- *Flexible multilayer switching support and forwarding architectures*—Select basic Layer 2 forwarding or feature-rich Cisco Express Forwarding (CEF) using the same supervisor

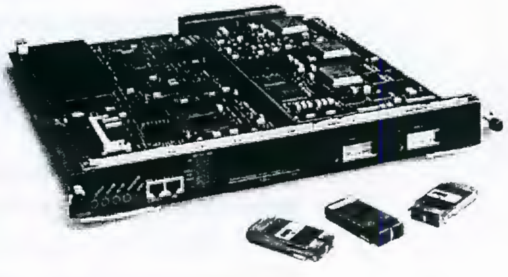
Cisco Systems, Inc.

- *Choice of operating system support*—Support both Cisco IOS® Software, Catalyst OS software, and Hybrid (Catalyst OS software and Cisco IOS Software for the MSFC)
- *Operational consistency*— Support all 3 generations of Catalyst 6500 Series interface and services modules in all Catalyst 6500 3-, 6-, 9- and 13-slot chassis running Cisco IOS® Software and Cisco Catalyst Operating System Software and a common set of Cisco network management tools that support the Catalyst 6500 Supervisor Engine 1A and 2 as well as many other Cisco Systems product lines
- *Maximum network uptime and user productivity*—Provide fault-tolerant network resilience and high availability features including fast 1- to 3-second stateful fail-over between redundant Catalyst 6500 supervisor engines enabling near-hitless software upgrades for business critical network environments, including IP-telephony enabled wiring closets
- *Extensive management tools*—Support CiscoWorks network management platform, Simple Network Management Protocol (SNMP) versions 1, 2, and 3 and four RMON groups (statistics, history, alarms, and events)

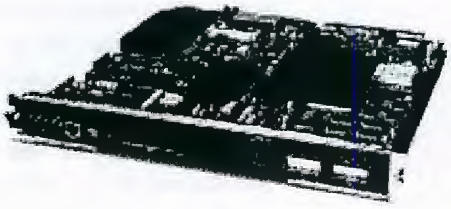
As part of the Catalyst 6500 Series of modular products, Supervisor Engines 1A and 2 share a common operating system and CLI—encouraging an end-to-end Catalyst 6500 Series solution for maximum operational consistency, common sparing, and minimized training requirements (Figure 1).

Figure 1 Supervisor Engines 1A and Supervisor Engine 2

Supervisor Engine 1-PFC



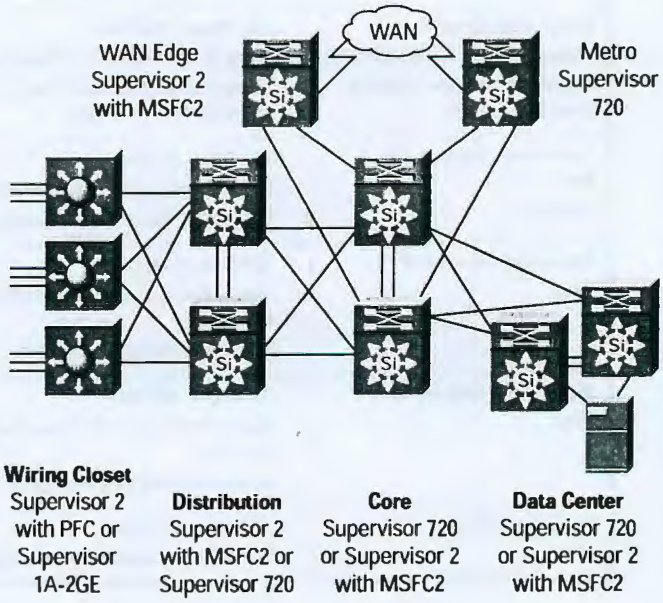
Supervisor Engine 2-MSFC2



Supervisor Engine 1A and Supervisor Engine 2 Deployment Scenarios

With a broad range of interfaces, and services modules, chassis / slot configurations as well as a scalable set of Supervisor Engines, the Catalyst 6500 can be deployed anywhere in the network. The figure below depicts the Catalyst 6500 deployed in the wiring closet, distribution, core, data center, WAN edge and Metro and provides recommended supervisor engines for each part of the network.

Figure 2
Cisco Supervisor Engine 1A and Supervisor Engine 2 Deployment Scenarios



The following table outlines the primary deployment scenarios for Cisco Catalyst 6500 Series supervisor engines.

Table 1 Deployment Scenarios for Cisco Catalyst 6500 Series Supervisor Engines

Supervisor Engine	Performance/Features	Recommended Deployments
Supervisor Engine 720	400 Mpps, 720 Gbps Layer 2–4 distributed Cisco Express Forwarding Supports new accelerated Cisco Express Forwarding 720 and distributed Cisco Express Forwarding 720 interface modules	Enterprise core, distribution, and data centers
Supervisor Engine 2 Policy Feature Card 2 (PFC2) Multilayer Switch Feature Card 2 (MSFC2)	210 Mpps, 256 Gbps Layer 2–4 distributed Cisco Express Forwarding Supports distributed Cisco Express Forwarding 256 interface modules	Enterprise distribution, data centers, and WAN edge
Supervisor Engine 1A PFC MSFC2	15 Mpps, 32 Gbps Centralized Layer 2–4 forwarding Enhanced security and quality of service (QoS)	Distribution and core
Supervisor Engine 2 PFC2	30 Mpps, 256 Gbps Centralized Layer 2 forwarding and Layer 3–4 services Enhanced security and QoS	Premium wiring closet and data center access
Supervisor Engine 1A PFC	15 Mpps, 32Gbps Centralized Layer 2 forwarding and Layer 3–4 services Enhanced security and QoS	Enterprise wiring closets
Supervisor Engine 1A 2GE	15 Mpps, 32 Gbps Centralized Layer 2 forwarding	Value wiring closet

Supervisor Engine 1A and 2 Features

The Supervisor Engine 1A and 2 provide the following features:

- High availability
- Scalable performance
- Wire-rate traffic management
- End-to-end management tools
- Comprehensive security
- Advanced Layer 2, Layer 3, and Layer 4 forwarding

High Availability

Supervisor Engines 1A and 2 can be deployed in dual-supervisor engine configurations in all Cisco Catalyst 6500 Series chassis (6503, 6506, 6509, and 6513). The dual-supervisor engine configuration synchronizes protocol states between the primary and the redundant supervisor engine, provides industry-leading network availability with sub-3-second failover, and maximizes network uptime by allowing hot swapping of standby supervisor engines. Important high-availability features include:

- *Supervisor engine redundancy*—With synchronization of protocol states and support for HSRP and Uplink Fast
- *Rapid failover rates*—Sub-3-second stateful failover and Layer 3 IP Unicast and Multicast failover
- *Hot swapping*—Hot swapping of standby supervisors

Scalable Performance

Supervisor Engines 1A and 2 provide scalable performance, from 15 Mpps to 210 Mpps with bandwidth scaling from 32 Gbps to 256 Gbps, that densely populated wiring closets and high-throughput network cores with multigigabit trunks require.

Supervisor Engine 2 uses the Cisco Express Forwarding routing architecture that performs high-speed lookups even with advanced Layer 3 services enabled, and independent of the number of flows through the switch, while maintaining 30 Mpps of centralized performance and 210 Mpps of distributed performance.

- *Supervisor Engine 1A*—Provides 15-Mpps performance with 32-Gbps bandwidth
- *Supervisor Engine 2*—Provides 30 Mpps of centralized performance and 210 Mpps of distributed performance with 256-Gbps bandwidth

For details see Table 2—Cisco Catalyst 6500 Supervisor Engine Feature Comparison.

Wire-Rate Traffic Management

Supervisor Engines 1A and 2 provide wire-rate traffic management using Layer 2, 3, and 4 QoS and security checks, including ACL policy enforcement, as part of their forwarding process to protect and secure content. These traffic management features enable efficient handling of converged networks that carry a mix of mission-critical, time-sensitive, and bandwidth-intensive multimedia applications.

- Advanced QoS tools such as packet classification and marking and congestion avoidance based on Layer 2, Layer 3, and Layer 4 header information.
- QoS scheduling rules with thresholds can be configured in the switch for multiple receive and transmit queues.
- Rate limiting can be used to police traffic on a per-flow or aggregate basis with a very fine granularity.

For details see Table 3—QoS Features Comparison.

End-to-End Management Tools

Managed with CiscoWorks2000, Cisco Catalyst 6500 Series switches can be configured and managed to deliver end-to-end device, VLAN, traffic, and policy management. Cisco Resource Manager, a Web-based management tool that works with CiscoWorks2000, provides: automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

Supervisor Engines 1A and 2 provide a comprehensive set of management tools to provide the required visibility and control in the network.

- *Console management*—Provide shared interface to the Supervisor Engine 2 and the Multilayer Switch Feature Card 2 (MSFC2) available out-of-band from a local terminal or remote terminal connected through a modem to the console or auxiliary interface
- *In-band management*—Provide shared interface to the Supervisor Engine 2 and the MSFC2 available in-band through SNMP, Telnet client, Bootstrap Protocol (BOOTP), and Trivial File Transfer Protocol (TFTP)
- *SPAN*—Allow management and monitoring of switch traffic
- *RSPAN*—Allow centralized management and monitoring by aggregating and directing traffic from multiple distributed hosts and switches to a remotely located switch through a trunk link
- *VACL Capture*—Direct traffic to a network analysis port using an ACL

For details see Table 4—Management Tools Comparison.

Comprehensive Security

The advanced security capabilities of Supervisor Engines 1A and 2 can reduce the threats of malicious attacks while enabling authentication, authorization, and accounting. With support for up to 32K ACL entries, IP/IPX security ACLs in hardware, and advanced features such as port security, Supervisor Engines 1A and 2 offer a superior set of Layer 2–4 network traffic security capabilities:

- *Layer 2 security features*—Include private VLANs and port security, to help the network architect properly partition and control the utilization of the switch resources.
- *Layer 2, 3, and 4 hardware filters*—Can work on the forwarding engine and in conjunction with optional integrated services modules to inspect each forwarded packet and permit or deny all the streams of traffic according to the network administrator's rules.

For details see Table 5—PFC and PFC2 Security Features Comparison.

Supervisor Engine 1A and 2 Architecture

Catalyst 6500 Series Supervisor Engines 1A and 2 manage the system by storing and running the system software, controlling the various modules in the chassis, performing basic forwarding, and providing the Gigabit uplinks that allow redundant supervisor engine connections.

Supervisor Engine 2 offers an improved forwarding design. The Supervisor Engine 1A CPU performs Layer 2 forwarding, but Supervisor Engine 2 performs Cisco Express Forwarding (CEF) and distributed CEF, doubling the forwarding performance. As shown in Table 2, Supervisor Engines 1A and 2 offer choices in operating characteristics, including forwarding architecture, performance, bandwidth, DRAM and boot Flash sizes, and support for chassis, Policy Feature Card/Policy Feature Card 2 (PFC/PFC2), MSFC2, and Switch Fabric Module (SFM).

Table 2 Cisco Catalyst 6500 Supervisor Engine Feature Comparison

Feature	**Supervisor Engine 2** ***Supervisor Engine-PFC2*** ***Supervisor Engine-MSFC2***	**Supervisor Engine 1A** ***Supervisor Engine 1A-2GE*** ***Supervisor Engine 1A-PFC*** ***Supervisor Engine 1A-/MSF***
Cisco Express Forwarding (CEF)	Yes	No
Performance	30 Mpps—*Supervisor Engine 2- PFC2 and Supervisor Engine 2-MSFC2* up to 210 Mpps—*Supervisor Engine 2- MSFC2 with SFM and DFCs*	15 Mpps
Maximum bandwidth	256 Gbps (with distributed forwarding)	32 Gbps
DRAM	128 MB, 256 MB, 512 MB	128 MB
Onboard Flash (BootFlash)	32 MB	16 MB
Chassis supported	6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A, 6513; 7603, 7606, 7609, OSR-7609, 7613	6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A; 7603, 7606, 7609, OSR-7609
PFC daughter card available	Yes (PFC2); Standard with Supervisor Engine 2	Yes (PFC); Not field upgradable
MSFC2 daughter card available	Yes, and field upgradable	Yes, not field upgradable
SFM supported	Yes	No

The PFC/PFC2 and MSFC2 daughter cards and the SFM increase Supervisor Engines 1A and 2 functions:

- *PFC and PFC2*—Perform hardware-based Layer 2, Layer 3, and Layer 4 packet forwarding as well as packet classification, traffic management, and policy enforcement
- *MSFC2*—Performs Layer 3 control plane functions including address resolution and routing protocols
- *SFM 2*—Provides 256 Gbps dedicated bandwidth to all slots in the chassis and requires Supervisor Engine 2-MSFC2. The SFM 2 will not operate in the same chassis with Supervisor Engine 720.

Policy Feature Card (PFC and PFC2)

The Policy Feature Card provides quality of service (QoS) and policy based intelligent networking capabilities to the Catalyst 6500 Series. Recommended for premier wiring closets, backbone, data center and WAN edge deployments, the PFC identifies and classifies traffic applying the appropriate QoS priority level and Security Policies as defined by the network administrator configured ACLs. The PFC also helps to prevent unauthorized applications from being allowed on the network.

The Supervisor Engine PFC daughter card makes the packet forwarding decision in its application-specific integrated circuit (ASIC) complex. In distributed forwarding implementations, an identical ASIC complex located on an interface module's DFC daughter card allows the interface module to make packet-forwarding decisions locally. After the PFC or DFC makes the forwarding decision for the interface module, it sends the forwarding result to the interface module that does all packet buffering, queuing, and delivery.

In addition to packet forwarding, the PFC performs the following major functions at wire-rate:

- *Layer 3 packet classification*—Using QoS access-control entries
- *Traffic management (rate limiting)*—Using ingress and egress policing
- *Security policy enforcement*—Within subnets or VLANs
- *Intelligent multicast forwarding*—Efficient replication of multicast streams, supplied to appropriate end-user stations
- *NetFlow data export*—Collecting IP flow statistics for inter-subnet flows

QoS

The following table shows the PFC and PFC2 QoS features.

Table 3 QoS Features Comparison

Feature	PFC2 *Supervisor Engine 2 PFC2* *Supervisor Engine 2 MSFC2*	PFC *Supervisor Engine 1A PFC* *Supervisor Engine 1A PFC/MSFC2*	No PFC *Supervisor Engine 1A-2GE*
Layer 2 classification and marking	Yes	Yes	Yes
Layer 3 classification and marking/ Access Control Entries (ACEs)	Yes 32K	Yes 16K	None
Rate limiting location (port)	Ingress port, VLAN	Ingress port, VLAN	None
Rate Limiting Level Types *CIR = Committed Information Rate* *PIR = Peak Information Rate*	CIR, PIR	CIR	None
Aggregate traffic rate limiting/ number of policers	Yes 1023 policers	Yes 1023 policers	None
Flow-based rate limiting method/ number of rates	Full flow; 64 rates	Full flow; 64 rates	None

Management Tools

The following table compares the management tools that are available with Supervisor Engines 1A and 2.

Table 4 Management Tools Comparison

Feature	PFC *Supervisor Engine 1A PFC* *Supervisor Engine 1A PFC/MSFC2* *Supervisor Engine 2 PFC2* *Supervisor Engine 2 MSFC2*	No PFC *Supervisor Engine 1A-2GE*
SPAN	Yes	Yes
RSPAN	Yes	No
ERSPAN	No	No
VACL Capture	Yes	No

Security

Table 5 shows the PFC and PFC2 security features.

Table 5 PFC and PFC2 Security Features Comparison

Feature	With PFC2 *Supervisor Engine 2 PFC2* *Supervisor Engine 2 MSFC2*	With PFC *Supervisor Engine 1A PFC* *Supervisor Engine 1A PFC/MSFC2*	Without PFC *Supervisor Engine 1A-2GE*
Port security	Yes	Yes	Yes
TCP intercept hardware acceleration	Yes	Yes	No
IEEE 802.1X and 802.1X extensions	Yes	Yes	No
IP security ACLs in hardware	Yes	Yes	No
IPX security ACLs in hardware	Yes	Yes	No
Security ACL entries	32K	16K	No
Reflexive ACLs	128K	512K	No
Unicast Reverse Path Forwarding (uRPF) check-in hardware	Yes	No	No
CPU rate limiters	1	None	None

Multi-layer Switch Fabric Card2 (MSFC2)

Supported on both Supervisor 1A and Supervisor 2 as an option the MSFC2 acts as the Layer 3 forwarding routing engine. On its Layer 3 forwarding routing engine, the MSFC2 builds the CEF Forwarding Information Base (FIB) table in software and then downloads this table to the ASICs on the PFC or DFC that make the forwarding decisions for IP Unicast and Multicast traffic. For more information see How Cisco Express Forwarding Works.

Layer 3 Switching

Table 6 shows the MSFC2 Layer 3 switching features.

Table 6 Layer 3 Switching Feature Comparisons

Feature	**MSFC2** ***Supervisor Engine 1A-PFC/MSFC2*** ***Supervisor Engine 2-MSFC2***	**No MSFC2** ***Supervisor Engine 2-PFC2***	**No MSFC2** ***Supervisor Engine 1A-2GE*** ***Supervisor Engine 1A-PFC***
IPv4 routing	Yes	Yes, with MSFC2 upgrade	No, not upgradable
MPLS	Yes, through OSM	Yes, through OSM	No
IPv6	Yes, in software (only on Supervisor Engine 2-MSFC2	No, requires MSFC2 upgrade	No

Note: Refer to the release notes for up-to-date software version information.

Switch Fabric Modules (SFM and SFM2)

Designed to support distributed forwarding, the Cisco Catalyst 6500 Series SFM (WS-X6500-SFM) and SFM2 (WS-X6500-SFM2) provide dedicated bandwidth to each slot up to 256 Gbps per system.

For distributed forwarding to work, an interface module must have a Distributed Forwarding Card (DFC) and must be installed in the chassis with either a Supervisor Engine 2-MSFC2 and an SFM or SFM2, or a Supervisor Engine 720. The SFM works with Cisco Catalyst 6506, 6509, 6509-NEB, and 6509-NEB-A chassis and can occupy any slot. The SFM2 works with 6506, 6509, 6509-NEB, 6509-NEB-A, 6513, 7603, 7606, 7609, OSR-7609, and 7613 chassis; and it can occupy any slot, except in the 6513 and 7613 where it must occupy slot 7 or 8.

The Catalyst 6503 does not currently support the SFM modules as this would leave one slot open after configuring the supervisor and SFM in two of the three available slots. However, the Supervisor 720 provides full CEF256, dCEF256, aCEF720 and dCEF720 capabilities to the Catalyst 6503 chassis with its slot-efficient integration of the supervisor engine and switch fabric in a single module.

Switch Fabric Module Architecture

Providing access to the switch fabric through dual 8-Gbps serial channels, the SFM or SFM2 performs all switching on the module independent of the passive backplane. For more information see How Distributed Cisco Express Forwarding (dCEF) Works.

High Availability

Two SFM and SFM2 modules can be configured in a system for high availability with 1-to-1 redundancy, where one SFM or SFM2 is operational and one serves as a backup.

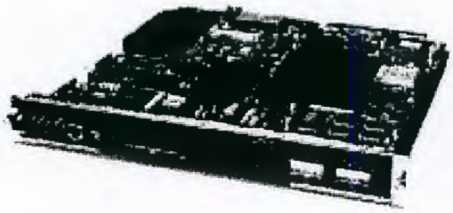
Note: The SFM and SFM2 cannot operate in the same chassis with a Supervisor Engine 720.

Supervisor Engine 2-MSFC2

Suited for deployment in the distribution/core with Classic interface modules, CEF256 interface modules and dCEF256 interface modules, Supervisor 1A-2GE provides Layer 2/3/4 forwarding with the following operational advantages:

- *Layer 2–4 forwarding*—Performs Layer 2 – 4 forwarding with Layer2, 3, 4 features; supports dCEF256 interface modules
- *Media Access Control (MAC) addresses*—128K
- *Forwarding rate*—Up to 30 Mpps per system
- *Bandwidth*—32 Gbps per system; 256 Gbps with SFM in chassis
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (See Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—IPv4 supported (See Table 6 for details)
- Distributed forwarding—Requires Switch Fabric Module and interface modules with Distributed Forwarding Cards (DFCs); for details, see section titled How Distributed Cisco Express Forwarding (dCEF) Works
- *Operating system*—Cisco Catalyst OS with Cisco IOS on the MSFC and Cisco IOS Software
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128, 256, 512 MB
- *Onboard flash (BootFlash)*—32 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A, and 6513; 7603, 7606, 7609, OSR-7609, and 7613
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—None required

Figure 3
Cisco Catalyst 6500 Series Supervisor Engine 2-MSFC2



Supervisor Engine 2-PFC2

Suited for deployment in wiring closets with Classic and CEF256 interface modules, Supervisor Engine 1A-2GE provides basic Layer 2 forwarding with the following operational advantages:

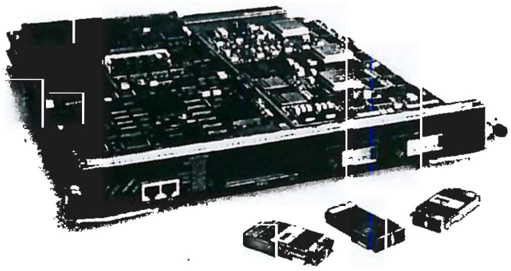
- *Layer 2 forwarding*—Performs Layer 2 forwarding with Layer2, 3, 4 features; requires MSFC2 upgrade to support Layer 3, 4 forwarding
- *MAC addresses*—128K
- *Forwarding rate*—Up to 30 Mpps per system
- *Bandwidth*—32 Gbps per system; 256 Gbps with SFM in chassis
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (See Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—Requires MSFC2 upgrade (See Table 6 for details)
- *Distributed forwarding*—Requires MSFC2 upgrade, SFM, and interface modules with DFCs (for details, see section titled How Distributed Cisco Express Forwarding (dCEF) Works).
- *Operating system*—Cisco Catalyst OS only (Cisco IOS Software supported with MSFC2 upgrade)
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128, 256, 512 MB
- *Onboard flash (BootFlash)*—32 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, 6509-NEB, 6509-NEB-A, and 6513; 7603, 7606, 7609, OSR-7609, and 7613
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—MSFC2 upgrade

Supervisor Engine 1A-PFC/MSFC2

Suited for deployment in the distribution/core with Classic interface modules, Supervisor Engine 1A-2GE provides Layer 2–4 forwarding with the following operational advantages:

- *Layer 2–4 forwarding*—Performs Layer 2–4 forwarding with Layer 2–4 features
- *MAC addresses*—128K
- *Forwarding rate*—Up to 15 Mpps per system
- *Bandwidth*—32 Gbps per system
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (see Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—IPv4 supported (See Table 6 for details)
- *Distributed forwarding*—Unsupported
- *Operating system*—Cisco Catalyst OS with Cisco IOS on the MSFC and Cisco IOS Software
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128 MB
- *Onboard flash (BootFlash)*—16 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, and 6509-NEB, 6509-NEB-A (6513 not supported); 7603, 7606, 7609, and OSR-7609 (7613 not supported)
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—None

Figure 4
Cisco Catalyst 6500 Supervisor Engine 1A-PFC/MSFC2



Cisco Systems, Inc.

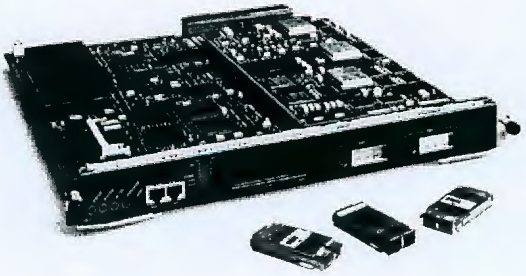
Supervisor Engine 1A-PFC

Suited for deployment in wiring closets with Classic interface modules, Supervisor Engine 1A-2GE provides basic Layer 2 forwarding with the following operational advantages:

- *Layer 2 forwarding*—Performs basic Layer 2 forwarding with no Layer 2–4 features
- *MAC addresses*—128K
- *Forwarding rate*—Up to 15 Mpps per system
- *Bandwidth*—32 Gbps per system
- *Layer 2, 3 traffic classification and marking*—Layer 2 and Layer 3 (See Table 3—QoS Features Comparison for details)
- *Multilayer (Layer 3) switching*—Unsupported
- *Distributed forwarding*—Unsupported
- *Operating system*—Cisco Catalyst OS only
- *Management tools*—SPAN, RSPAN, VACL capture
- *DRAM*—128 MB
- *Onboard flash (BootFlash)*—16 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, and 6509-NEB, 6509-NEB-A (6513 not supported); 7603, 7606, 7609, and OSR-7609 (7613 not supported)
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrades*—None

Figure 5

Cisco Catalyst 6500 Supervisor Engine 1A-PFC



Supervisor Engine 1A-2GE

Suited for deployment in wiring closets with Classic interface modules, Supervisor Engine 1A-2GE provides basic Layer 2 forwarding with the following operational advantages:

- *Layer 2 forwarding*—Performs Layer 2 forwarding with Layer 4 features
- *MAC addresses*—128K
- *Forwarding rate*—Up to 15 Mpps per system
- *Bandwidth*—32 Gbps per system
- *Layer 2, 3 traffic classification and marking*—Layer 2 only, not upgradable to support Layer 3 (for details, see Table 3—QoS Features Comparison)
- *Multilayer (Layer 3) switching*—Unsupported
- *Distributed forwarding*—Unsupported
- *Operating system*—Cisco Catalyst OS only
- *Management tools*—SPAN only
- *DRAM*—64 MB
- *Onboard flash (BootFlash)*—16 MB
- *Chassis supported*—Cisco Catalyst 6006, 6009, 6503, 6506, 6509, and 6509-NEB, 6509-NEB-A (6513 not supported); 7603, 7606, 7609, and OSR-7609 (7613 not supported)
- *Slot requirements*—Slots 1 or 2 of any chassis
- *Upgrade support*—None

How Cisco Express Forwarding Works

Cisco Express Forwarding (CEF) is a Layer 3 technology that provides increased forwarding scalability and performance to handle many short-duration traffic flows common in today's enterprise and service provider networks. To meet the needs of environments handling large amounts of short-flow, Web-based, or highly interactive types of traffic, CEF forwards all packets in hardware, and maintains its forwarding rate completely independent of the number of flows going though the switch.

On the Cisco Catalyst 6500 Series, the CEF Layer 3 forwarding engine is located centrally on the supervisor engine's PFC2 or PFC3—the same device that performs hardware-based Layer 2 and 3 forwarding, ACL checking, QoS policing and marking, and NetFlow statistics gathering.

Using the routing table that Cisco IOS Software builds to define configured interfaces and routing protocols, the CEF architecture creates CEF tables and downloads them into the hardware-forwarding engine before any user traffic is sent through the switch. The CEF architecture places only the routing prefixes in its CEF tables—the only information it requires to make the Layer 3 forwarding decisions—relying on the routing protocols to do route selection. By performing a simple CEF table lookup, the switch forwards packets at wire-rate, independent of the number of flows transiting the switch.

CEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 2 or Catalyst Supervisor Engine 720.

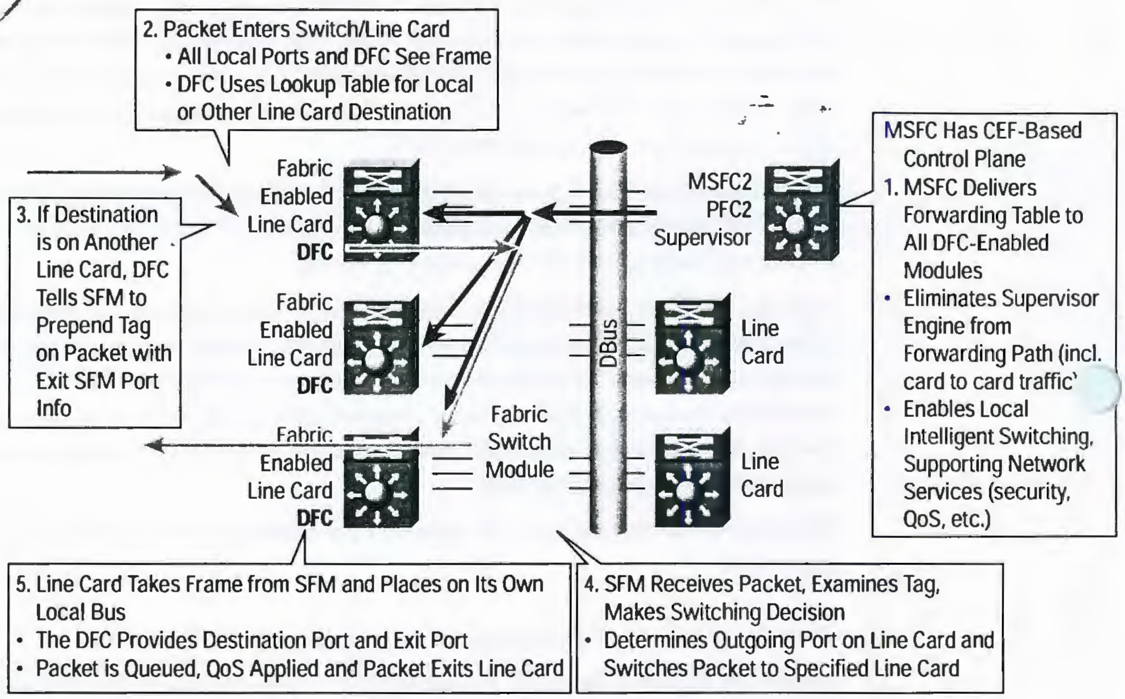
How Distributed Cisco Express Forwarding (dCEF) Works

With Distributed Cisco Express Forwarding (dCEF), forwarding engines located on the interface modules make forwarding decisions locally and in parallel, allowing the Cisco Catalyst 6500 Series to achieve the highest forwarding rates in the industry. With dCEF, forwarding occurs on the interface modules in parallel and system performance scales up to 400 Mpps—the aggregate of all forwarding engines working together.

Using the same ASIC engine design as the central PFCx, DFCs located on the interface modules forward packets between two ports, directly or across the switch fabric, without involving the supervisor engine. With the DFC, each interface module has a dedicated forwarding engine complete with the full forwarding tables. dCEF forwarding works like this:

- As in standard CEF forwarding, the central PFC3 located on the supervisor engine and the DFC engines located on the interface modules are loaded with the same CEF information derived from the forwarding table before any user traffic arrives at the switch.
- As a packet arrives at an interface module, its DFC engine inspects the packet and uses the information in the CEF table (including Layer 2, Layer 3, ACLs, and QoS) to make a completely hardware-based forwarding decision for that packet.
- The dCEF engine handles all hardware-based forwarding for traffic on that module, including Layer 2 and Layer 3 forwarding, ACLs, QoS policing and marking, and NetFlow.
- Because the DFCs make all the switching decisions locally, the supervisor engine is freed from all forwarding responsibilities and can perform other software-based functions, including routing, management, and network services.

Figure 5
Distributed Cisco Express Forwarding Packet Flow


Fabric Enabled Line Card DFC
Fabric Enabled Line Card DFC
Fabric Enabled Line Card DFC
Fabric Switch Module
DBus
MSFC2 PFC2 Supervisor
Line Card
Line Card

2. Packet Enters Switch/Line Card
- All Local Ports and DFC See Frame
- DFC Uses Lookup Table for Local or Other Line Card Destination

3. If Destination is on Another Line Card, DFC Tells SFM to Prepend Tag on Packet with Exit SFM Port Info

MSFC Has CEF-Based Control Plane
1. MSFC Delivers Forwarding Table to All DFC-Enabled Modules
- Eliminates Supervisor Engine from Forwarding Path (incl. card to card traffic'
- Enables Local Intelligent Switching, Supporting Network Services (security, QoS, etc.)

5. Line Card Takes Frame from SFM and Places on Its Own Local Bus
- The DFC Provides Destination Port and Exit Port
- Packet is Queued, QoS Applied and Packet Exits Line Card

4. SFM Receives Packet, Examines Tag, Makes Switching Decision
- Determines Outgoing Port on Line Card and Switches Packet to Specified Line Card

dCEF-based forwarding requirements: Requires a Cisco Catalyst Supervisor Engine 720 for dCEF720 interface modules; requires either a Catalyst Supervisor Engine 720 or a Catalyst Supervisor Engine 2-MSFC2 and a SFM for dCEF256 interface modules.

Software Requirements

Depending on its configuration, a supervisor engine will operate with one or more of the following operating systems:

- Cisco IOS Software for the supervisor engine (native Cisco IOS Software)
- Cisco Catalyst OS software
- Hybrid, Catalyst OS software and Cisco IOS Software for the MSFC

Notes: Refer to the release notes for up-to-date software version information.

Ordering Information

Table 7 lists the ordering information for the Supervisor Engines 1A and 2.

Table 7 Product Numbers for Ordering

Product Number	Description
WS-X6K-SUP1A-2GE	Catalyst 6500 Supervisor Engine1A, 2GE
WS-X6K-SUP1A-PFC	Catalyst 6500 Supervisor Engine1A, 2GE, plus PFC
WS-X6K-S1A-MSFC2	Catalyst 6500 Supervisor Engine1A, 2GE, plus MSFC-2 and PFC
WS-X6K-S2-PFC2	Catalyst 6500 Supervisor Engine 2, 2GE, plus PFC-2
WS-X6K-S2-MSFC2	Catalyst 6500 Supervisor Engine 2, 2GE, plus MSFC-2/PFC-2
WS-X6K-S1A-MSFC2	Supervisor Engine 1A with PFC+MSFC2
WS-X6K-S1A-MSFC2=	Supervisor Engine 1A with PFC+MSFC2=
WS-X6K-S1A-MSFC2/2	Supervisor Engine 1A with PFC+MSFC2/2
WS-F6K-MSFC2	Catalyst 6500 Multilayer Switch Feature Card 2
MEM-MSFC2-128MB=	Catalyst 6500 MSFC2 Memory, 128 MB DRAM Spare
MEM-MSFC2-256MB	Catalyst 6500 MSFC2 Memory, 256 MB DRAM Option
MEM-MSFC2-256MB=	Catalyst 6500 MSFC2 Memory, 256 MB DRAM Spare
MEM-MSFC2-512MB	Catalyst 6500 MSFC2 Memory, 512 MB DRAM Option
MEM-MSFC2-512MB=	Catalyst 6500 MSFC2 Memory, 512 MB DRAM Spare
WS-X6500-SFM	Catalyst 6500 Switch Fabric Module
WS-X6500-SFM2	Catalyst 6500 Switch Fabric Module2

Dimensions

- (H x W x D): 1.6 x 15.3 x 16.3 in. (4.0 x 37.9 x 40.3 cm)

Environmental Conditions

- Operating temperature: 32 to 104 F (0 to 40 C)
- Storage temperature: –40 to 167 F (–40 to 75 C)
- Relative humidity: 10 to 90%, noncondensing
- Regulatory compliance

Safety Certifications

- UL 1950
- EN 60950
- CSA-0C22.2 No. 950
- IEC 950

Electromagnetic Emissions Certifications

- FCC 15J Class A
- VCCI CE II
- CE mark
- EN 55022 Class B
- CISPR 22 Class B

Technical Support Services

Whether your company is a large organization, a commercial business, or a service provider, Cisco Systems is committed to maximizing the return on your network investment. Cisco offers a portfolio of Technical Support Services to ensure that your Cisco products operate efficiently, remain highly available, and benefit from the most up-to-date system software.

Cisco Technical Support Services offers the following features, which help enable network investment protection and minimal downtime for systems running mission-critical applications:

- Provides Cisco networking expertise online and on the telephone
- Creates a proactive support environment with software updates and upgrades as an ongoing integral part of your network operations, not merely a remedy when a failure or problem occurs
- Makes Cisco technical knowledge and resources available to you on demand
- Augments the resources of your operations technical staff to increase productivity
- Complements remote technical support with onsite hardware replacement
- The Cisco portfolio of Technical Support Services includes:
- Cisco SMARTnet™ support
- Cisco SMARTnet Onsite support
- Cisco Software Application Services, including Software Application Support and Software Application Support plus Upgrades

For more information visit:

http://www.cisco.com/en/US/products/svcs/ps3034/serv_category_home.html

E C T
7.095
A.
L. AC
I

Additional Cisco Catalyst 6500 Series Information

For additional information about the Cisco Catalyst 6500 Series, supervisor engines, interface modules, SFM, and services modules, visit:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_data_sheets_list.html

- Catalyst 6500 Series Data Sheet
- Catalyst 6500 Supervisor Engine 720 Data Sheet
- Catalyst 10/100 and 10/100/1000 Ethernet Data Sheet
- Catalyst 6500 Gigabit Ethernet Interface Modules Data Sheet
- Catalyst 6500 10 Gigabit Ethernet Interface Modules Data Sheet
- Catalyst 6500 FlexWAN Interface Modules Data Sheet
- Catalyst 6500 Switch Fabric Interface Modules Data Sheet
- Catalyst 6500 Content Services Module (CSM) Data Sheet
- Catalyst 6500 Firewall Services Module Data Sheet
- Catalyst 6500 Network Application Module (NAM) Data Sheet
- Catalyst 6500 Intrusion Detection (IDS) Module Data Sheet
- Catalyst 6500 IP Sec/VPN Services Module Data Sheet
- Catalyst 6500 SSL Services Module Data Sheet

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

203070/ETMG 07/03

Apêndice FG

CHAPTER 3

Installing the Switch

Note In this publication, the term Catalyst 6500 series refers only to the switch chassis listed in Table 1-1. The Catalyst 6000 series switches are described in a separate publication, the *Catalyst 6000 Series Switch Installation Guide.*

This chapter describes how to install a Catalyst 6500 series switch in a rack. For first-time installations, perform the procedures in the following sections in the order listed:

- Unpacking the Switch, page 3-3
- Installing the Rack-Mount Kit, page 3-3
- Installing the Switch Chassis in the Rack, page 3-15
- Installing the Stabilizer Kit (Catalyst 6509-NEB and Catalyst 6513 Switches Only), page 3-19
- Establishing the System Ground, page 3-22
- Installing the Power Supplies in the Switch Chassis, page 3-26
- Attaching the Interface Cables, page 3-26
- Verifying Switch Chassis Installation, page 3-36

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.**

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.**

Warning **This equipment must be installed and maintained by service personnel as defined by AS/NZS 3260. Incorrectly connecting this equipment to a general-purpose outlet could be hazardous. The telecommunications lines must be disconnected 1) before unplugging the main power connector or 2) while th housing is open, or both.**

Warning **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.**

Caution During this procedure, wear a grounding wrist strap to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.

Note If you are installing a free-standing (not rack-mounted) Catalyst 6509-NEB or Catalyst 6513 switch, you must install the stabilizer kit, which is part of the accessory kit for these two switches.

Before starting the installation procedures in this chapter, see the "Site Preparation Checklist" section on page 2-20 to verify that all site planning activities were completed.

For information on installing modules, refer to the *Catalyst 6500 Series Switch Module Installation Guide*.

Unpacking the Switch

Tip Do not discard the shipping container when you unpack the switch. Flatten the shipping cartons and store them with the pallet. You will need these containers if you need to move or ship the switch in the future. Repacking instructions are provided in Appendix C, "Repacking the Switch."

Perform the following to check the contents of the shipping container:

- Check the contents of the accessory kit against the Accessory Kit Components Checklist and the packing slip. Verify that you received all listed equipment, which should include the following:
  - Switch hardware and software documentation, if ordered
  - Optional equipment that you ordered, such as network interface cables, transceivers, or special connectors
- Check the switching modules in each slot. Ensure that the configuration matches the packing list and that all the specified interfaces are included.

Installing the Rack-Mount Kit

This section describes how to install the rack-mount kit. The kit contains a shelf bracket and crossbar assembly that attaches directly to the rack.

The Catalyst 6500 series chassis also have L brackets that are used to secure the chassis to the rack. Normally, the Catalyst 6500 series chassis are shipped with the L brackets installed. This section also contains procedures for installing the L brackets, for instances in which the chassis are not shipped with the L brackets installed.

Open the rack-mount kit, and use the checklist in Table 3-1 to verify that all parts are included.

Table 3-1 Rack-Mount Kit Contents Checklist

Part Description	Received
2 L brackets[1]	
M3 Phillips countersunk-head screws	
M4 Phillips countersunk-head screws[2]	
12-24 x 3/4-inch Phillips binder-head screws	
10-32 x 3/4-inch Phillips binder-head screws	
2 Shelf brackets	
1 Crossbar bracket	
M3 Phillips pan-head screws	

[1] The Catalyst 6500 series chassis are normally shipped with the L brackets installed.

[2] The M4 Phillips countersunk-head screws are included only in the accessories kits for the Catalyst 6509-NEB and Catalyst 6513 switch chassis. The M4 screws are for use with those two chassis only.

Rack-Mounting Guidelines

Before rack-mounting the switch, ensure that the equipment rack complies with the following guidelines:

- The width of the rack, measured between the two front mounting strips or rails, must be 17.75 inches (45.09 cm).
- The depth of the rack, measured between the front and rear mounting strips, must be at least 19.25 inches (48.9 cm) but not more than 32 inches (81.3 cm).
- The rack must have sufficient vertical clearance to insert the chassis. The chassis heights are as follows:
  - Catalyst 6503 switch—7 inches (17.8 cm) (4 RU)
  - Catalyst 6506 switch—20.1 inches (50.1 cm) (12 RU)
  - Catalyst 6509 switch—25.5 inches (64.8 cm) (15 RU)

- Catalyst 6509-NEB switch—33.5 inches (85.1 cm) (20 RU)
- Catalyst 6513 switch—33.0 inches (83.8 cm) (19 RU)

Note Chassis height is sometimes measured in rack units (RU).

Caution If the rack is on wheels, ensure that the brakes are engaged or that the rack is otherwise stabilized.

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.**

Note We recommend that you maintain a minimum air space of 6 inches (15 cm) between walls and the chassis air vents and a minimum horizontal separation of 12 inches (30.5 cm) between two chassis to prevent overheating.

This rack-mounting kit is not suitable for use with racks that have obstructions (such as power strips) because the obstructions could impair access to switch field-replaceable units (FRUs).

Required Tools

These tools and equipment are required to install the rack-mount kit:

- Number 1 and number 2 Phillips screwdrivers
- 3/16-inch flat-blade screwdriver
- Tape measure and level

Installing the Shelf Brackets and Crossbar Bracket

To install the shelf bracket and crossbar bracket, follow these steps:

Step 1 Position one of the two shelf brackets in the rack as shown in Figure 3-1.

Step 2 Secure the shelf bracket to the rack by using three 12-24 x 3/4-inch or 10-32 x 3/4-inch screws.

Step 3 Repeat Steps 1 and 2 for the second shelf bracket. Make sure that the second shelf bracket is level with the first bracket.

Step 4 Attach the crossbar bracket to the back of the shelf brackets using two M3 screws as shown in Figure 3-2.

Figure 3-1 Installing the Shelf Brackets

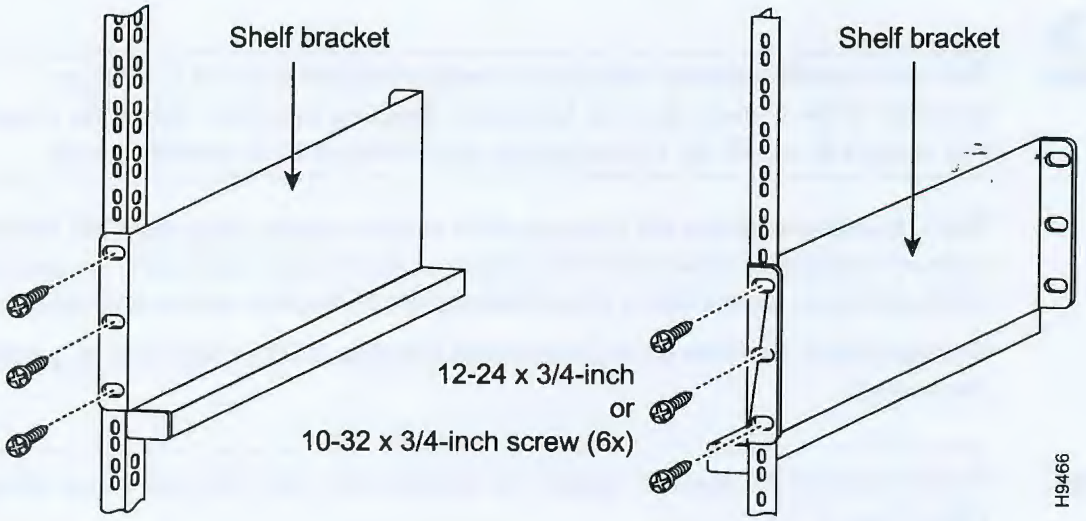
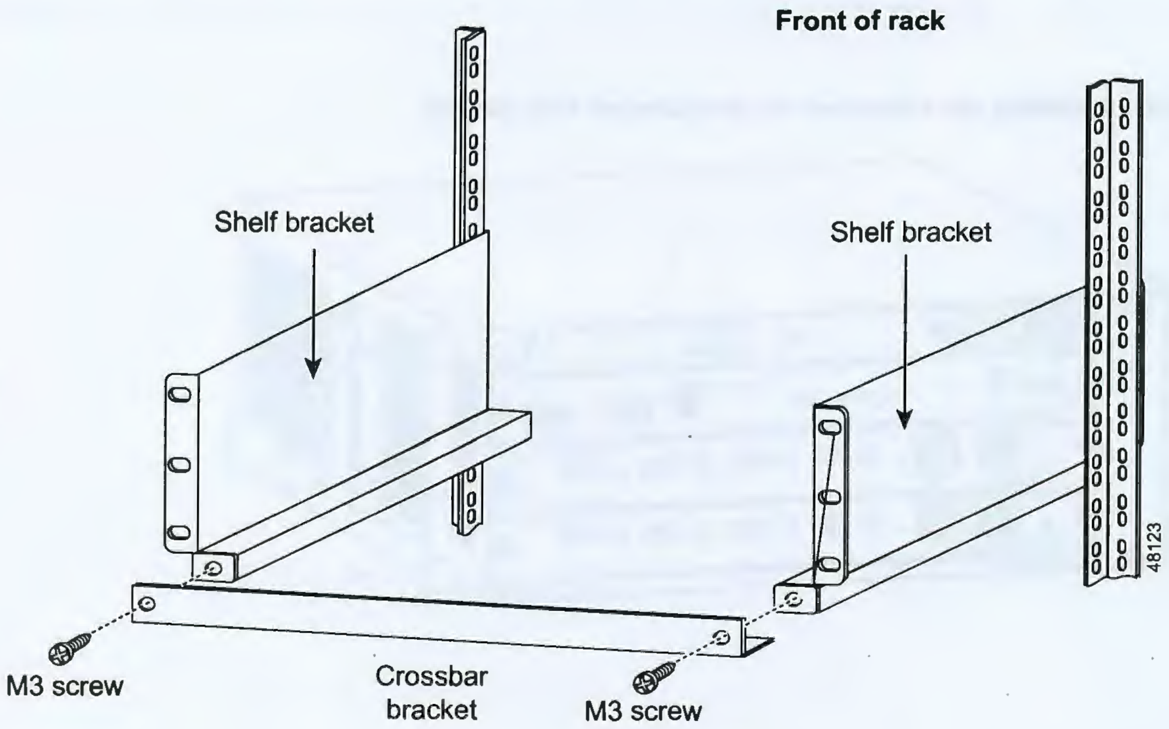


Figure 3-2 Attaching the Crossbar Bracket to the Shelf Brackets



Installing the L Brackets on the Catalyst 6503 Switch

Note The Catalyst 6503 switch chassis is normally shipped with the L brackets installed. If the chassis does not have the L brackets installed, follow the steps in this section to install the L brackets on your Catalyst 6503 switch chassis.

The L brackets attach to the Catalyst 6503 switch chassis using eight M3 Phillips countersunk-head screws (four M3 screws on each side). You attach the optional cable guides by sandwiching them between the L brackets and switch chassis.

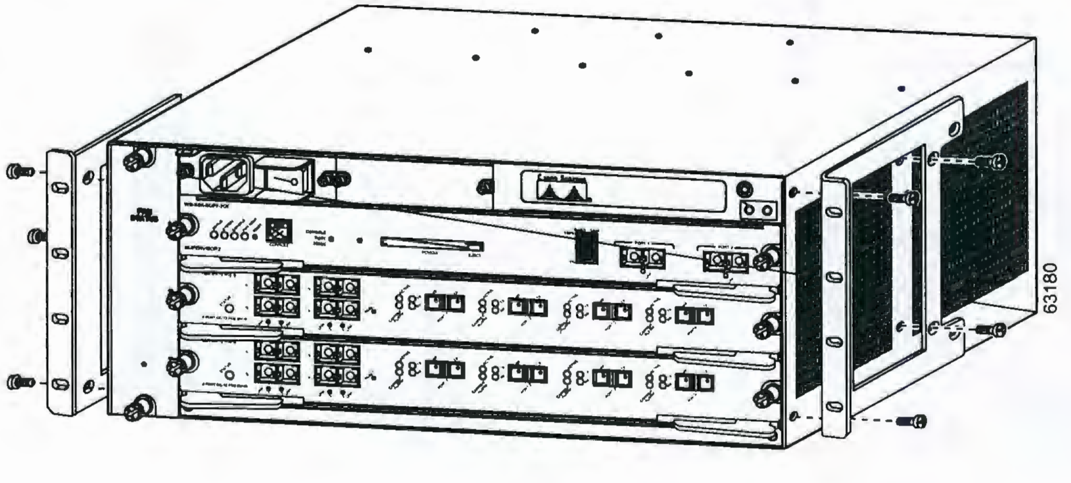
To install the L brackets on the front of the Catalyst 6503 switch chassis, perform these steps:

Step 1 Position one of the brackets against the chassis side, and align the screw holes. (See Figure 3-3.)

Step 2 Secure the bracket to the chassis with four screws.

Step 3 Repeat Steps 1 and 2 for the other bracket.

Figure 3-3 Installing the L-Brackets on the Catalyst 6503 Switch



Installing the L Brackets and Cable Guides on the Catalyst 6506 Switch

Note The Catalyst 6506 switch chassis is normally shipped with the L brackets installed. If the chassis does not have the L brackets installed, follow the steps in this section to install the L brackets on your Catalyst 6506 switch chassis.

The L brackets attach to the Catalyst 6506 switch chassis using eight M3 Phillips countersunk-head screws (four M3 screws on each side). You attach the optional cable guides by sandwiching them between the L brackets and the switch chassis.

Note The L brackets for the Catalyst 6506 switches are stamped with an L and an R to identify them as left and right.

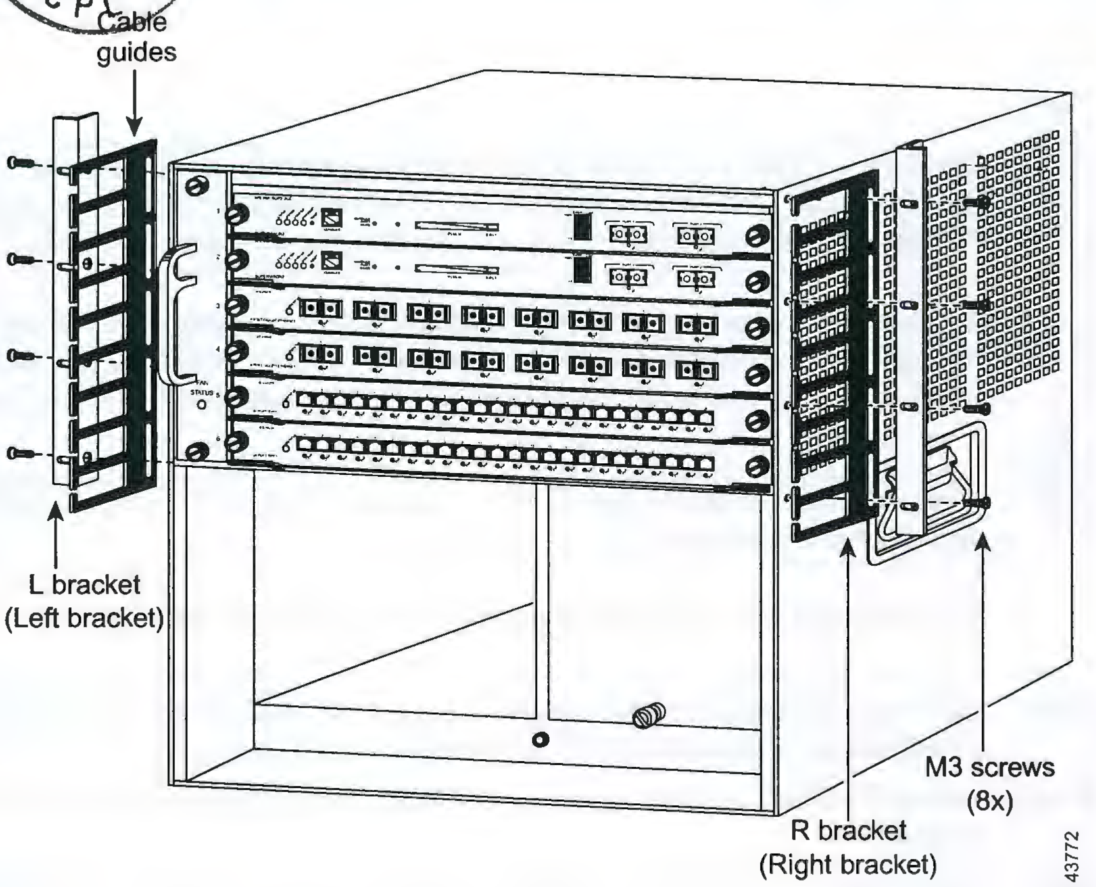
To install the L brackets and optional cable guides, follow these steps:

Step 1 Position the left (L) L bracket and the optional cable guide (if desired) against the switch chassis side, and align the screw holes. (See Figure 3-4.)

Step 2 Secure the L bracket (and optional cable guide) to the switch chassis with four M3 screws.

Step 3 Repeat steps 1 and 2 for the right (R) L bracket (and, if necessary, the optional cable guide).

Figure 3-4 Attaching L Brackets and Cable Guides: Catalyst 6506 Switch



Installing the L Brackets and Cable Guides on the Catalyst 6509 Switch

Note The Catalyst 6509 switch chassis is normally shipped with the L brackets installed. If the chassis does not have the L brackets installed, follow the steps in this section to install the L brackets on your Catalyst 6509 switch chassis.

The L brackets attach to the Catalyst 6509 switch chassis using ten M3 Phillips countersunk-head screws (five screws on each side). You attach the optional cable guides by sandwiching them between the L brackets and switch chassis.

Note The L brackets for the Catalyst 6509 switches are stamped with an L and an R to identify them as left and right.

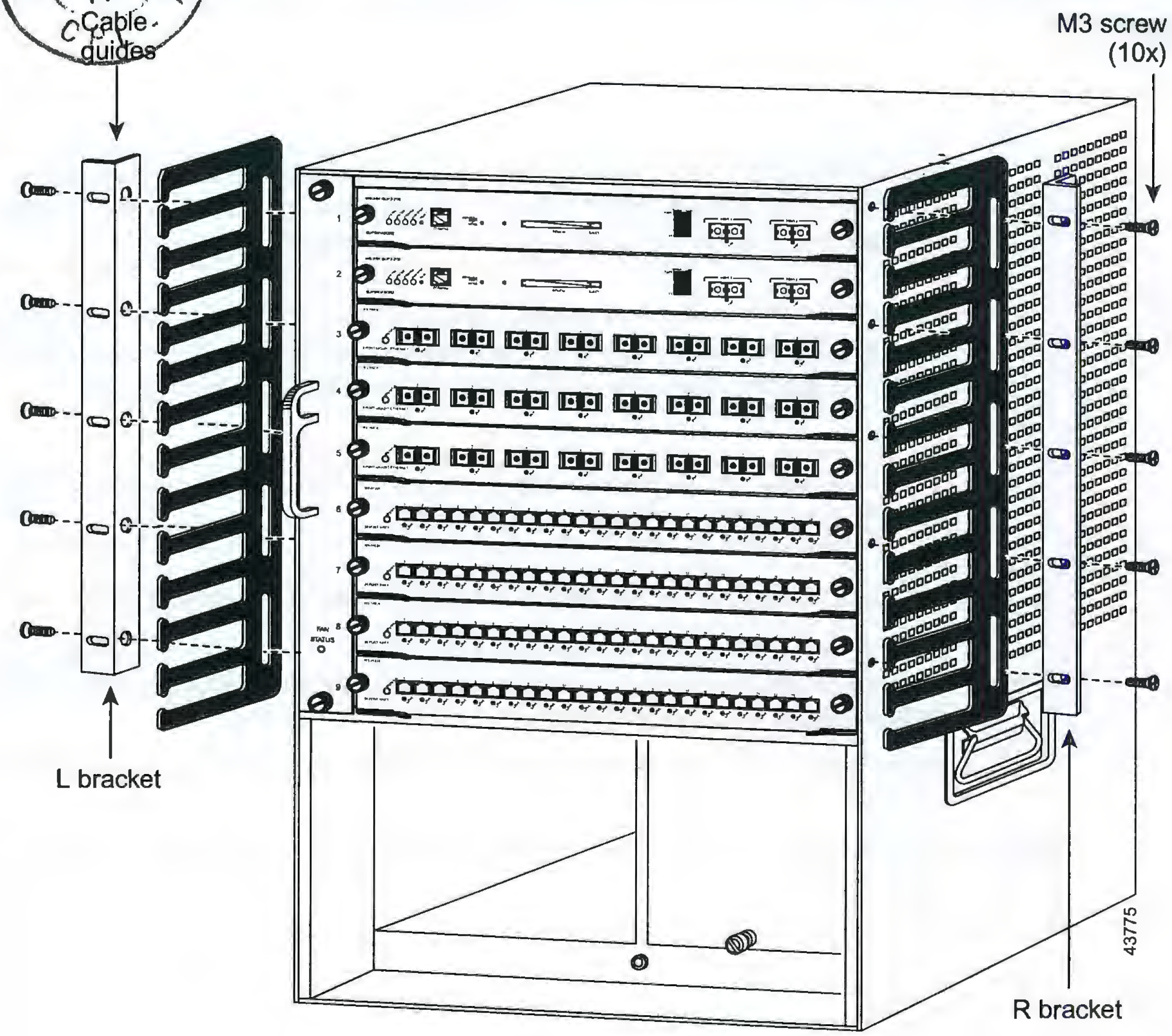
To install the L brackets and optional cable guides, follow these steps:

Step 1 Position the left (L) L bracket and the optional cable guide (if desired) against the switch chassis side, and align the screw holes. (See Figure 3-5.)

Step 2 Secure the L bracket (and optional cable guide) to the switch chassis with five M3 screws.

Step 3 Repeat steps 1 and 2 for the right (R) L bracket (and, if necessary, the optional cable guide).

Figure 3-5 Attaching L Brackets and Cable Guides: Catalyst 6509 Switch



Installing the L Brackets and Cable Guides on the Catalyst 6509-NEB Switch

Note The Catalyst 6509-NEB switch chassis is normally shipped with the L brackets installed. If the chassis does not have the L brackets installed, follow the steps in this section to install the L brackets on your Catalyst 6509-NEB switch chassis.

The Catalyst 6509-NEB L bracket screw holes are stamped + and –. You can install the brackets either on the left or right side of the chassis; use the + holes on one side and the – holes on the other side. The L brackets are installed with ten M4 Phillips countersunk-head screws (five screws on each side).

The optional cable guide installs on the front of the chassis and is secured with four M4 screws. To install the L brackets, follow these steps:

Step 1 Position one of the L brackets against the switch chassis side, and align the screw holes (use either the + or the – holes).

Step 2 Secure the L bracket to the switch chassis with five M4 screws.

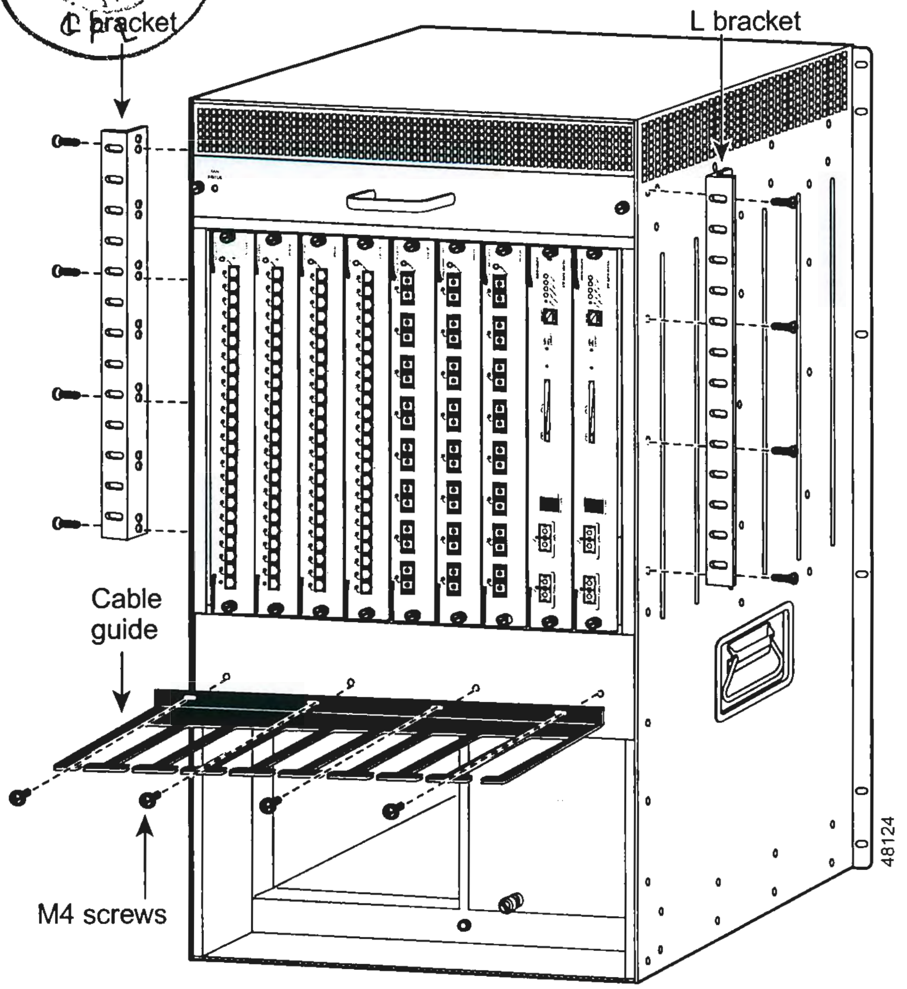
Step 3 Repeat steps 1 and 2 for the other L bracket. If you used the + set of holes for the first L bracket, use the – set of holes for the second L bracket.

To install the optional cable guide, follow these steps:

Step 1 Position the cable guide against the front of the chassis, and align the four screw holes as shown in Figure 3-6.

Step 2 Secure the cable guide with four M4 screws.

Figure 3-6 Attaching L Brackets and Cable Guides: Catalyst 6509-NEB Switch



Installing the Switch Chassis in the Rack

Note If you are not installing the Catalyst 6509-NEB switch or Catalyst 6513 switch in the rack, see "Installing the Stabilizer Kit (Catalyst 6509-NEB and Catalyst 6513 Switches Only)" section on page 3-19.

You are now ready to install the switch chassis in the rack.

Tip We recommend that you have a third person to assist in this procedure.

Caution Two people are required to lift the chassis. Grasp the chassis underneath the lower edge and lift with both hands. To prevent injury, keep your back straight and lift with your legs, not your back.

To install the switch chassis in the equipment rack, follow these steps:

Step 1 With a person standing at each side of the chassis, grasp the chassis handle with one hand and use the other hand near the back of the chassis for balance. Slowly lift the chassis in unison. Avoid sudden twists or moves to prevent injury.

Step 2 Position the chassis in the rack as follows (as shown in Figure 3-7):

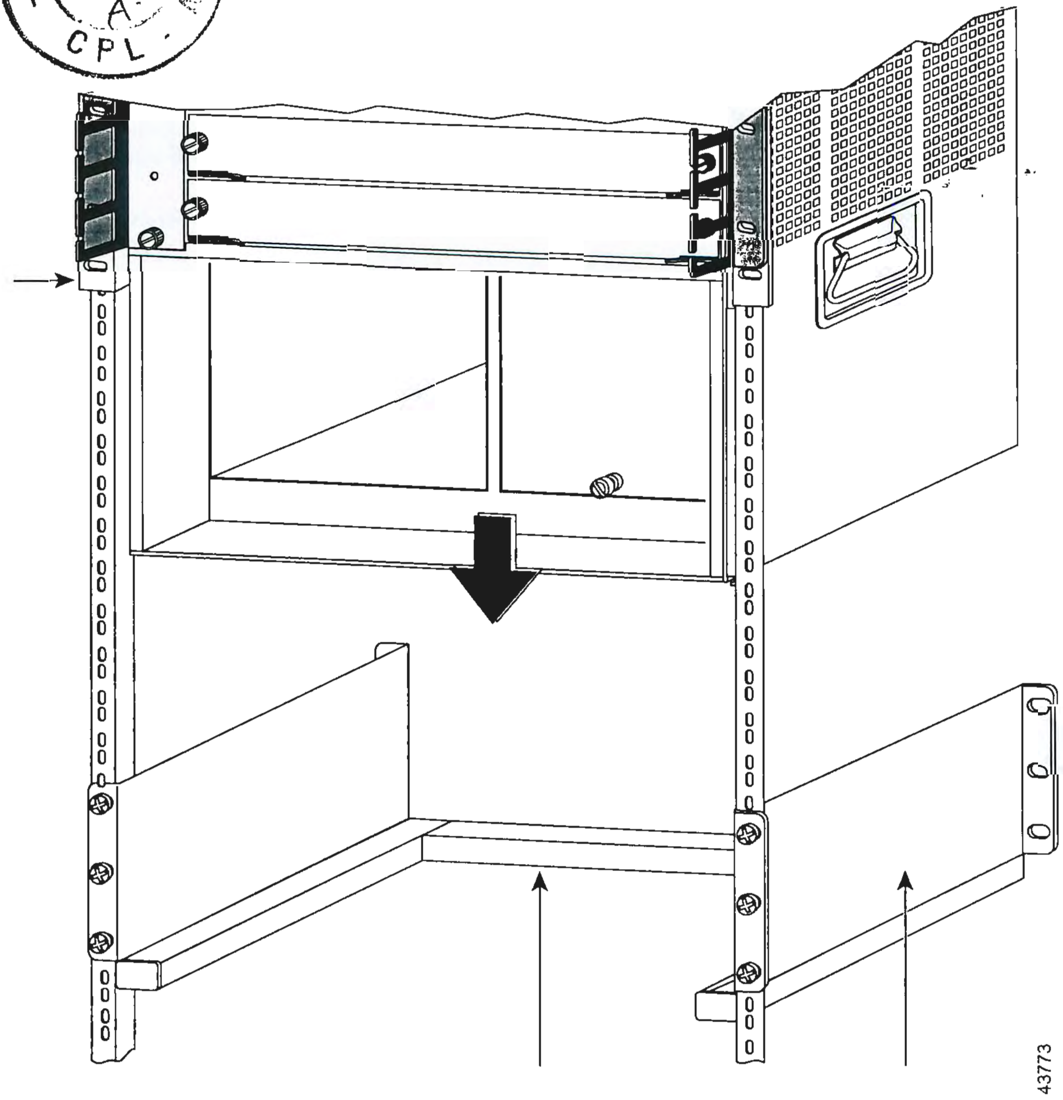
a. If the front of the chassis (front panel) is at the front of the rack, insert the rear of the chassis between the mounting posts.

b. If the rear of the chassis is at the front of the rack, insert the front of the chassis between the mounting posts.

Step 3 Rest the switch chassis on the shelf brackets and crossbar bracket.

Step 4 Align the mounting holes in the L bracket with the mounting holes in the equipment rack.

Figure 3-7 Installing the Switch in the Rack



Note If you are rack-mounting the Catalyst 6513 switch and you want to install the optional cable guides, perform Step 5; if not, go to Step 6.

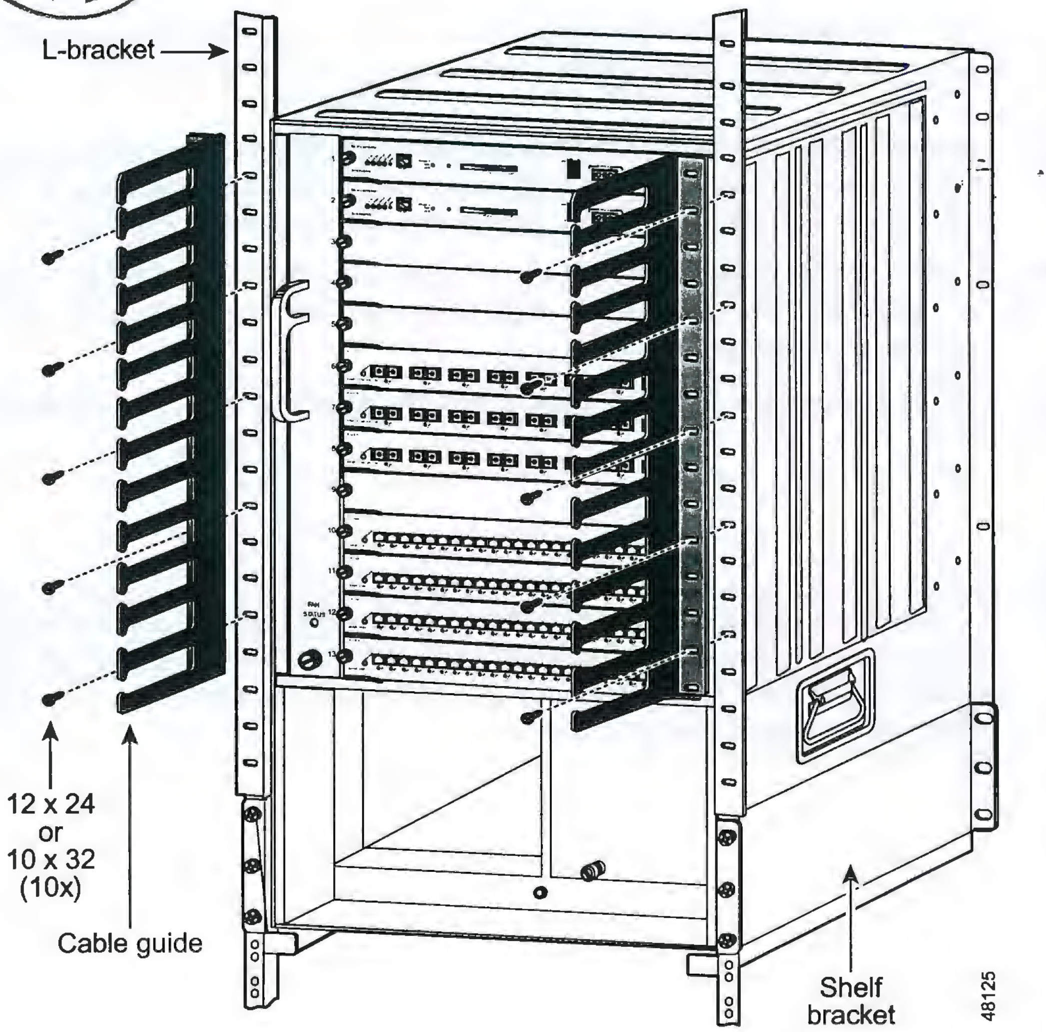
Step 5 Align the cable guide bracket mounting holes with the mounting holes in the L bracket and the mounting holes in the equipment rack and install ten (five per side) 12-24 x 3/4-inch or 10-32 x 3/4-inch screws as shown in Figure 3-8.

Step 6 Install the eight or ten (four or five per side) 12-24 x 3/4-inch or 10-32 x 3/4-inch screws through the holes in the L bracket and into the threaded holes in the equipment rack posts.

Step 7 Use a tape measure and level to verify that the chassis is installed straight and level.

Note If you are not rack-mounting the Catalyst 6513 switch and you are installing the optional cable guide assemblies, you must obtain ten 12x24 or 10x32 nuts. Use the screws supplied in the accessory kit and the nuts you obtained to attach the cable guide assembly to the L bracket.

Figure 3-8 Installing the Catalyst 6513 Switch in the Rack with the Optional Cable Guides



Installing the Stabilizer Kit (Catalyst 6509-NEB and Catalyst 6513 Switches Only)

Note The stabilizer kit is included only in the accessory kits for the Catalyst 6509-NEB and the Catalyst 6513 switches.

If you are not installing the Catalyst 6509-NEB or Catalyst 6513 switch in a rack, you must install stabilizer brackets to the bottom of the chassis. The stabilizer brackets reduce the possibility of the freestanding switch chassis tipping over.

Open the stabilizer kit package and use the kit contents list in Table 3-2 to verify that all parts are included.

Table 3-2 Stabilizer Kit Contents

Quantity	Part Description	Received
16	M4 Phillips countersunk-head screws	
2	Stabilizer brackets	

Note Have a second person available to perform the installation.

To install the stabilizer brackets, follow these steps:

Step 1 Have one person tilt and hold the chassis to one side.

Step 2 With the chassis tilted, attach the stabilizer bracket to the side of the chassis with the eight M4 screws as shown in Figure 3-9.

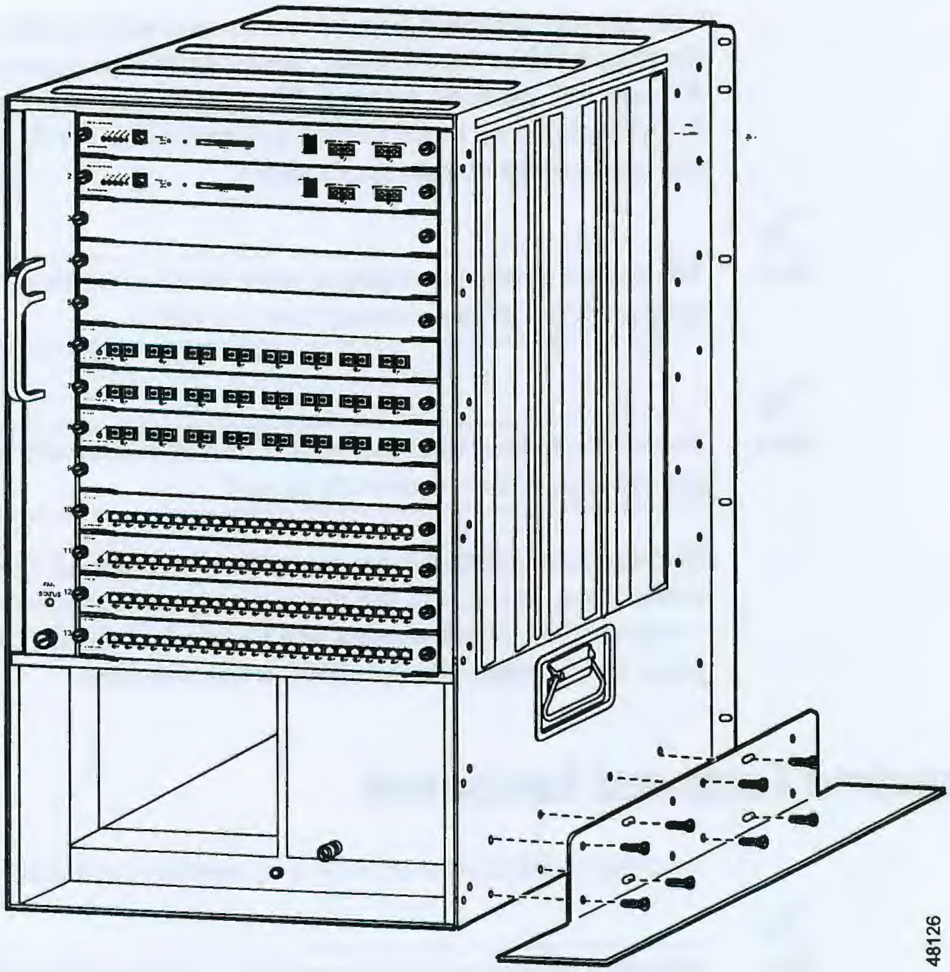
Step 3 Tilt the chassis to the other side.

Step 4 Attach the second stabilizer bracket to the other side of the chassis with eight M4 screws.

Step 5 Lower the chassis so that it rests on both stabilizer brackets.

Note If you are not rack-mounting the Catalyst 6513 switch and you want to install the cable guide assemblies, you must obtain ten 12x24 or 10x32 nuts. Use the screws supplied in the accessory kit and the nuts you obtained to attach the cable guide assembly to the L bracket.

Figure 3-9 Installing the Stabilizer Brackets



Establishing the System Ground

This section describes how to connect a system (earth) ground to the Catalyst 6500 series switches. You must use the system (earth) ground on both AC- and DC-powered systems. The system ground provides additional grounding for EMI shielding requirements and grounding for the low voltage supplies (DC-DC converters) on the modules.

Note The system ground connection must be installed along with any other rack or system power ground connections you make.

Note You must connect both the system ground connection and the power supply ground connection to an earth ground.

Two threaded M4 holes are provided on the chassis frame to attach the ground cable. (See Figure 3-10 for the system ground attachment point for the Catalyst 6503 switch chassis and Figure 3-11 for the system ground attachment point for the other Catalyst 6500 series switches.)

Required Tools and Equipment

To connect the system ground, you need the following tools and materials:

Note Materials are not provided; contact any commercial cable vendor for the required parts.

- Grounding lug—The grounding lug must have two M4 screw holes and accept 6 AWG wire.
- Two M4 (metric) hex-head screws with locking washers.

- One grounding wire—The grounding wire should be sized according to local and national installation requirements. The length of the grounding wires depends on the proximity of the switch to proper grounding facilities.
- Number 2 Phillips screwdriver.
- Crimping tool.
- Wire-stripping tool.

Connecting the System Ground

You must complete this procedure before connecting system power or turning on the Catalyst 6500 series switch.

To attach the grounding lug and cable to the grounding pad, follow these steps:

Step 1 Use a wire-stripping tool to remove approximately 0.75 inch (19 mm) of the covering from the end of the grounding wire.

Step 2 Insert the stripped end of the grounding wire into the open end of the grounding lug.

Step 3 Use a crimping tool to secure the grounding wire in place in the grounding lug.

Step 4 Locate and remove the adhesive label from the system grounding pad on the switch.

Step 5 Place the grounding wire lug against the grounding pad, making sure there is solid metal-to-metal contact.

Step 6 Secure the grounding lug to the chassis with two M4 screws. (See Figure 3-10 for the Catalyst 6503 switch or Figure 3-11 for the other Catalyst 6500 series switches.) Ensure that the grounding lug will not interfere with other switch hardware or rack equipment.

Step 7 Prepare the other end of the grounding wire and connect it to an appropriate grounding point in your site to ensure adequate earth ground for the switch.

Figure 3-10 Catalyst 6503 System Ground Connection

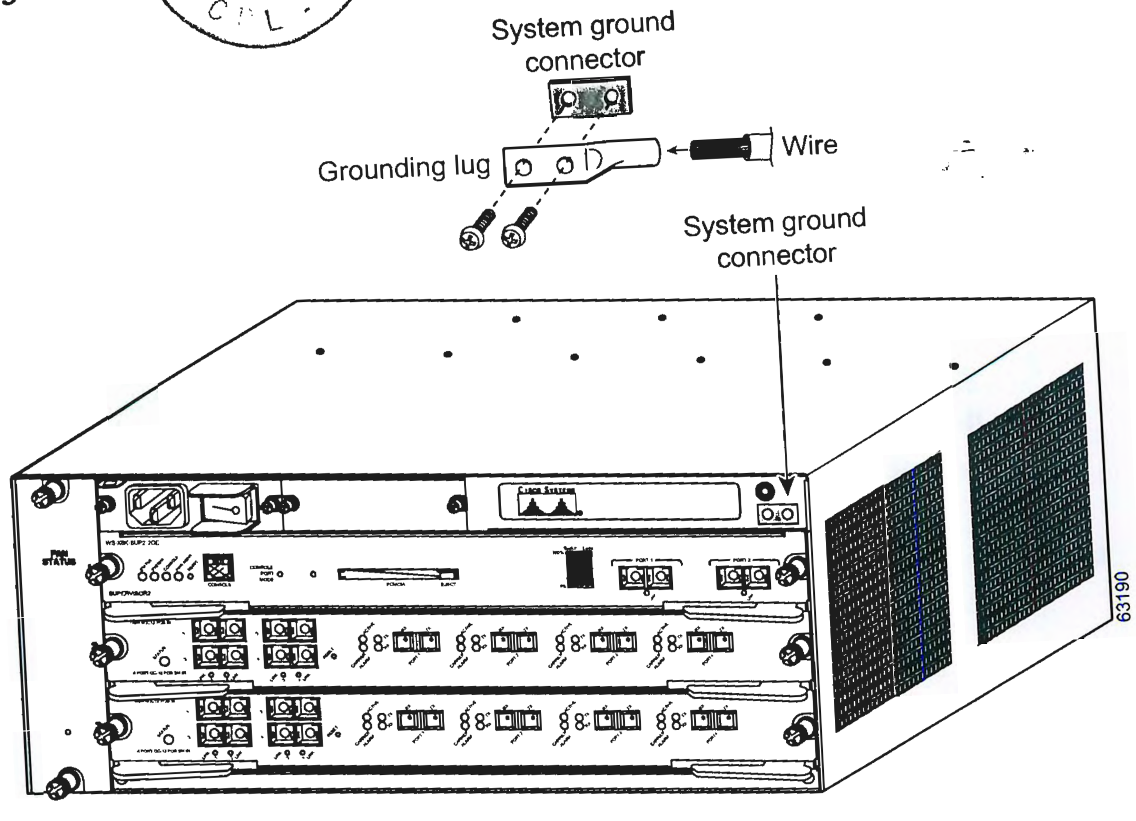
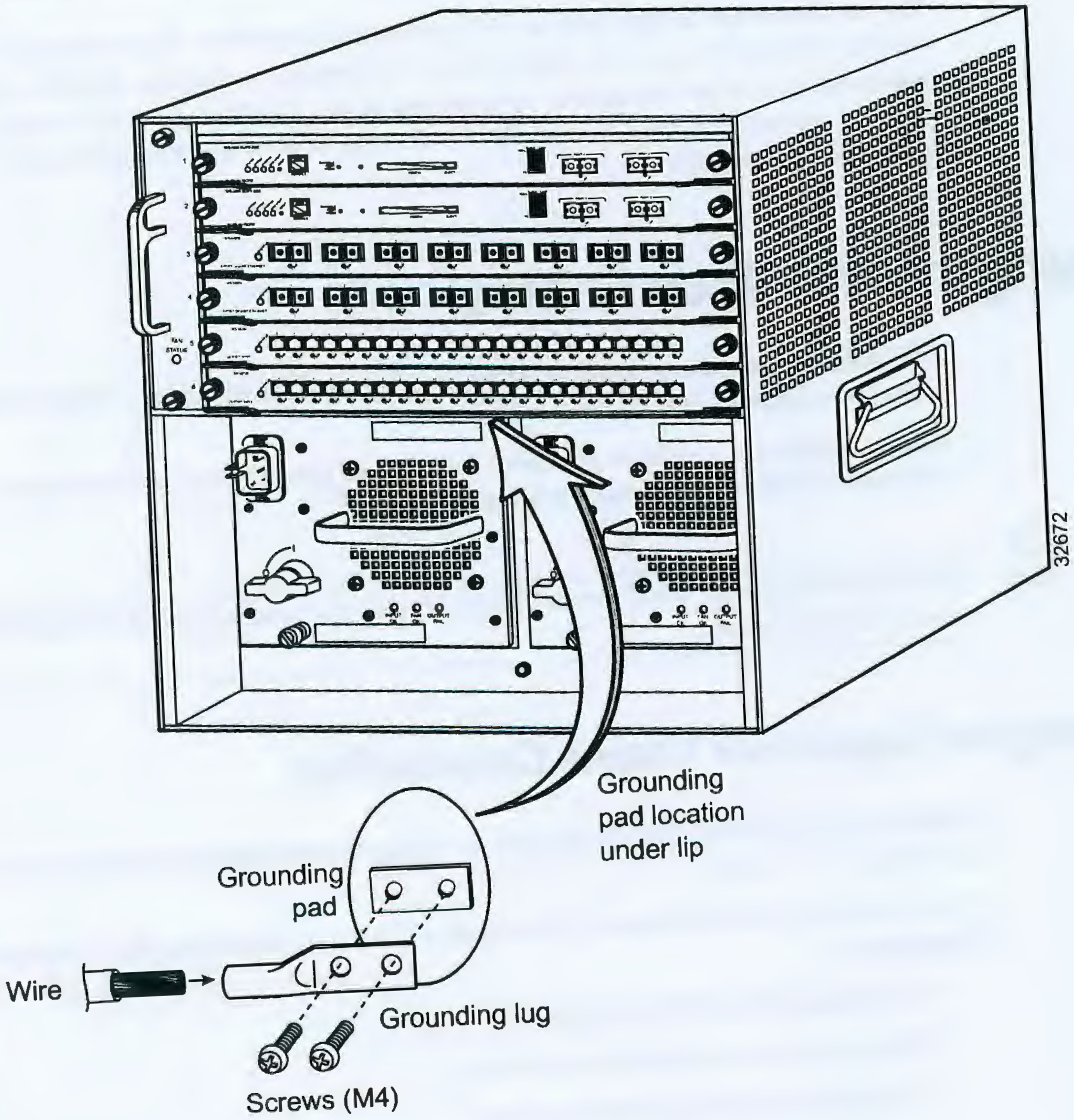


Figure 3-11 System Ground Location



Installing the Power Supplies in the Switch Chassis

The switch power supply (AC or DC) is shipped separately from the switch chassis. Remove the power supply from its shipping packaging, and then install and connect it to the site power by referring to the "Installing an AC-Input Power Supply" section on page 5-23 or the "Installing a DC-Input Power Supply" section on page 5-31.

Attaching the Interface Cables

This section provides general information on attaching interface cables to the supervisor engines and to the modules.

Depending on the modules you have installed in your chassis, you will have different styles of connectors to attach.

Note Refer to the *Catalyst 6500 Series Switch Module Installation Guide* for additional module information.

Connecting the Supervisor Engine Console Port

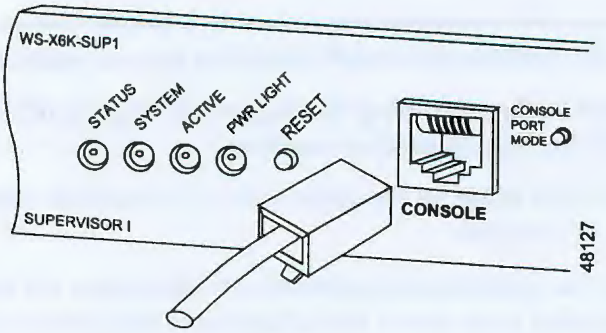
This section describes how to connect to the supervisor engine console port from a terminal or modem.

The console port on the supervisor engine allows you to perform the following functions:

- Configure the switch from the CLI
- Monitor network statistics and errors
- Configure SNMP agent parameters
- Download software updates to the switch or distribute software images residing in Flash memory to attached devices

The console port, located on the front panel of the supervisor engine, is shown in Figure 3-12.

Figure 3-12 Supervisor Engine Console Port Connector



Note The accessory kit that shipped with your Catalyst 6500 series switch contains the necessary cable and adapters to connect a terminal or modem to the console port.

To connect a terminal to the console port using the cable and adapters provided, follow these steps:

Step 1 Place the console port mode switch in the *in* position (factory default).

Step 2 Connect to the port using the RJ-45-to-RJ-45 cable and RJ-45-to-DB-25 DTE adapter or RJ-45-to-DB-9 DTE adapter (labeled "Terminal").

Step 3 Position the cable in the cable guide (if installed). Make sure there are no sharp bends in the cable.

Step 4 Check the terminal documentation to determine the baud rate. The baud rate of the terminal must match the default baud rate (9600 baud) of the console port. Set up the terminal as follows:

- 9600 baud
- 8 data bits
- No parity
- 2 stop bits

To connect a terminal using a Catalyst 5000 family Supervisor Engine III console cable, follow these steps:

Step 1 Place the console port mode switch in the *out* position.

Step 2 Connect to the port using the Supervisor Engine III cable and the appropriate adapter for the terminal connection.

Step 3 Position the cable in the cable guide (if installed). Make sure there are no sharp bends in the cable.

Step 4 Check the terminal documentation to determine the baud rate. The baud rate of the terminal must match the default baud rate (9600 baud) of the console port. Set up the terminal as follows:

- 9600 baud
- 8 data bits
- No parity
- 2 stop bits

To connect a modem to the console port, follow these steps:

Step 1 Place the console port mode switch in the *in* position.

Step 2 Connect to the port using the RJ-45-to-RJ-45 rollover cable and the RJ-45-to-DB-25 DCE adapter (labeled "Modem").

Step 3 Position the cable in the cable guide (if installed). Make sure there are no sharp bends in the cable.

Connecting the Supervisor Engine Uplink Ports

This section describes how to connect to the supervisor engine uplink ports.

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Note In a redundant configuration with two supervisor engines, the uplink ports on the redundant (standby) supervisor engine are active and can be used for normal traffic, like any other ports in the chassis.

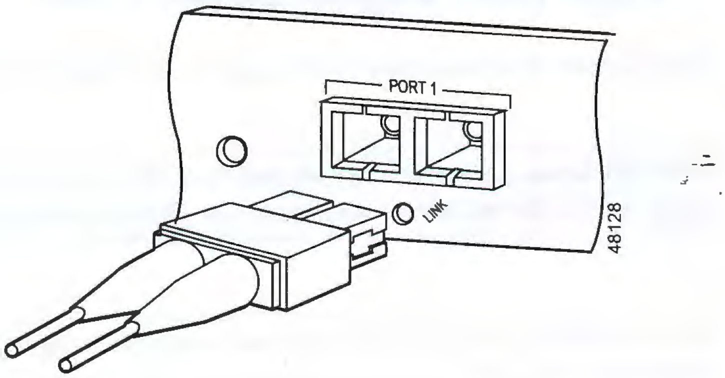
To connect to the supervisor engine uplink ports that use GBICs, follow these steps:

Step 1 Install the GBIC following the installation procedure contained in the *Gigabit Interface Converter Installation Note*.

Step 2 Remove the plugs from the Gigabit Interface Converter (GBIC) optical bores; store them for future use.

Step 3 Remove the plugs from the SC connector on the fiber-optic cable. Insert the connector into the GBIC. (See Figure 3-13.)

Figure 3-13 Connecting the Supervisor Engine Uplink Ports



Note When you plug the SC connector into the GBIC, make sure that both the transmit (Tx) and receive (Rx) fiber-optic cables are fully inserted into the SC connector.

Note If you are using the LX/LH GBIC with MMF, you need to install a patch cord between the GBIC and the MMF cable.

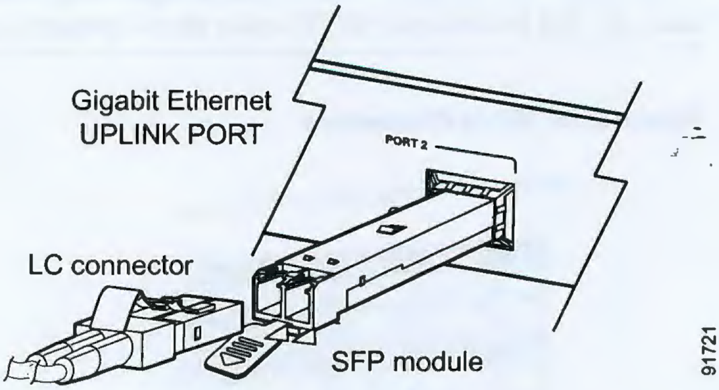
To connect to the supervisor engine uplink ports that use SFPs (Supervisor Engine 720), follow these steps (see Figure 3-14):

Step 1 Install the SFP module following the installation procedure contained in the *Cisco Small Form-Factor Pluggable Modules Installation Notes*.

Step 2 Remove the plug from the SFP optical bore; store it for future use.

Step 3 Remove the plug from the MT-RJ or LC connector on the fiber-optic cable. Insert the connector into the SFP.

Figure 3-14 Supervisor Engine 720 SFP Uplink Port



Connecting a Module

The Catalyst 6500 series modules use the following types of connectors:

- RJ-45
- RJ-21
- SC
- MT-RJ

RJ-45

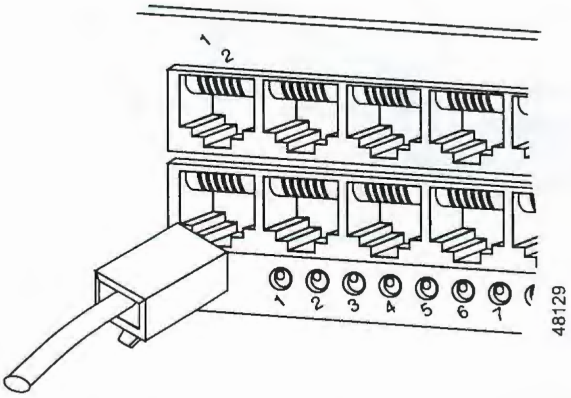
To connect to 10/100BASE-T or 1000BASE-T RJ-45 interfaces, use Category 3, Category 5, Category 5e, or Category 6 UTP or FTP cables with RJ-45 connectors, as shown in Figure 3-15. Connector pinouts are located in Appendix B.

⚠ **Caution** Category 5e and Category 6 cables can store large levels of static electricity because of the dielectric properties of the materials used in their construction. Always ground the cables (especially in new cable runs) to a suitable and safe earth ground before connecting them to the module.

T
7. 062
A.

Caution To comply with GR-1089 intrabuilding, lightening immunity requirements, you must use foil twisted-pair (FTP) cable that is properly grounded at both ends.

Figure 3-15 RJ-45 Connectors

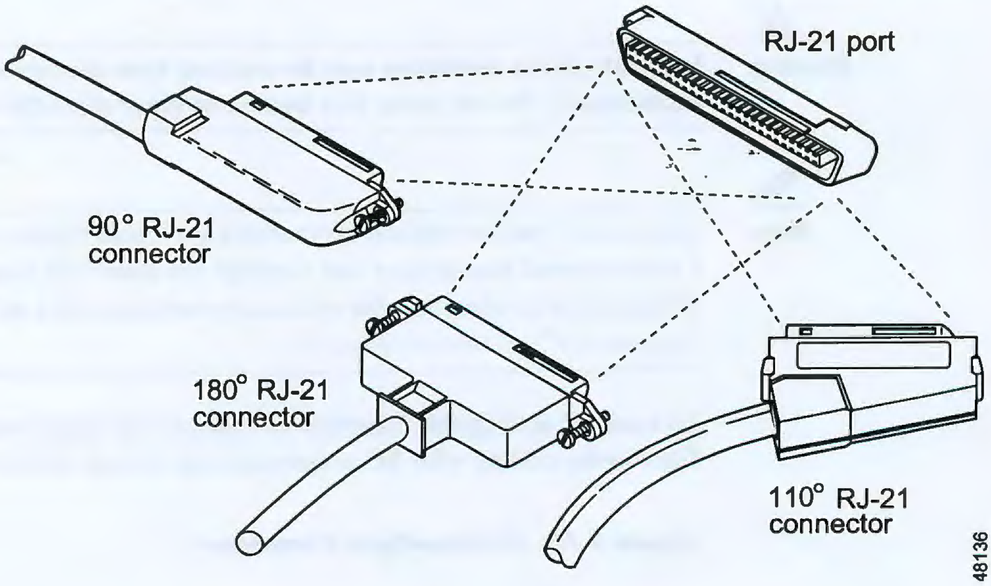


RJ-21

Warning **If the symbol of suitability with an overlaid cross appears above a port, you must not connect the port to a public network that follows the European Union standards. Connecting the port to this type of public network can cause severe personal injury or can damage the unit.**

To connect to 10/100BASE-TX RJ-21 telco interfaces, use Category 5 UTP cables with male RJ-21 connectors, as shown in Figure 3-16. The WS-X6224-FXS analog interface module also uses an RJ-21 connector, but the pinout arrangement is different than the 10/100BASE-TX.

Figure 3-16 RJ-21 Connectors



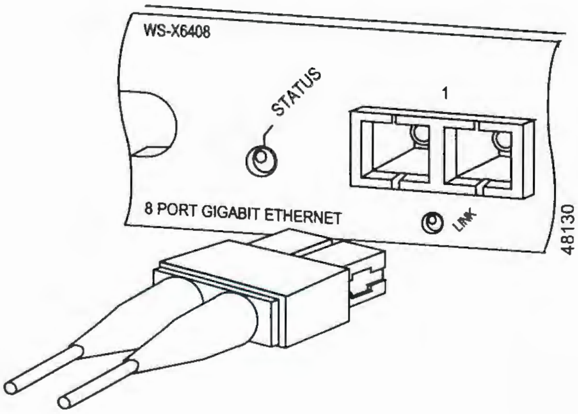
SC

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Note Make sure that the optical connectors are clean before making the connections. Contaminated connectors can damage the fiber and cause data errors. For information on cleaning the optical connectors, refer to "Cleaning the Fiber Optic Connectors" section on page B-11.

To connect to Gigabit Ethernet interfaces, use single-mode or multimode fiber-optic cables with SC connectors, as shown in Figure 3-17.

Figure 3-17 SC Fiber-Optic Connector



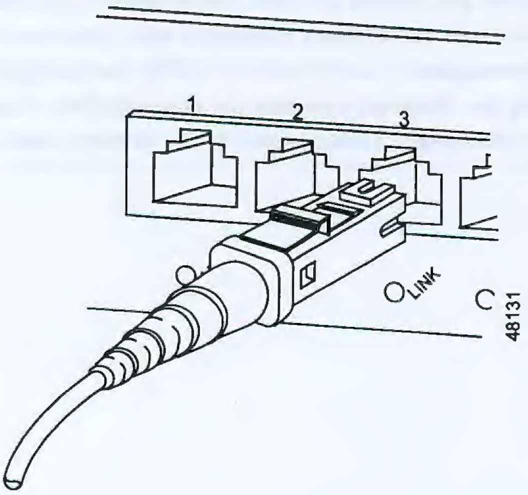
MT-RJ

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Note Make sure that the optical connectors are clean before making the connections. Contaminated connectors can damage the fiber and cause data errors. For information on cleaning the optical connectors, refer to "Cleaning the Fiber Optic Connectors" section on page B-11.

To connect to 100BASE-FX MT-RJ interfaces, use multimode fiber-optic cables with MT-RJ connectors, as shown in Figure 3-18.

Figure 3-18 MT-RJ Connector



Verifying Switch Chassis Installation

To verify the switch chassis installation, follow these steps:

Step 1 Verify that the ejector levers of each module are fully closed (parallel to the faceplate) to ensure that the supervisor engine and all switching modules are fully seated in the backplane connectors.

Step 2 Check the captive installation screws of each module, the power supply, and the fan assembly. Tighten any loose captive installation screws.

Step 3 Verify that all empty module slots have blank faceplates (WS-X6K-SLOT-CVR) installed and that the screws holding the plates in place are tight.

Step 4 Turn on the power supply switches to power up the system.

⚠ **Warning** **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.**

Apêndice FH

Product Overview

This chapter describes the Catalyst 6500 series switches and contains these sections:

- Catalyst 6503 Switch, page 1-2
- Catalyst 6506 Switch, page 1-4
- Catalyst 6509 Switch, page 1-7
- Catalyst 6509-NEB Switch, page 1-11
- Catalyst 6513 Switch, page 1-14
- System Features, page 1-17
- Fan Assembly, page 1-19
- Power Supplies, page 1-24

The Catalyst 6500 series switch chassis are listed in Table 1-1.

Table 1-1 Catalyst 6500 Series Switches

Catalyst 6500 Series Switch	Orientation/Number of Slots
Catalyst 6503	Horizontal 3-slot
Catalyst 6506	Horizontal 6-slot
Catalyst 6509	Horizontal 9-slot
Catalyst 6509-NEB	Vertical 9-slot
Catalyst 6513	Horizontal 13-slot

Note In this publication, the term Catalyst 6500 series refers only to the switch chassis listed in Table 1-2. The Catalyst 6000 series switches (Catalyst 6006 switch and Catalyst 6009 switch) are described in a separate publication, the *Catalyst 6000 Series Switches Installation Guide.*

Note Throughout this publication, except where noted, the term *supervisor engine* is used to refer to Supervisor Engine 1, Supervisor Engine 2, and Supervisor Engine 720.

Catalyst 6503 Switch

The Catalyst 6503 switch is a 3-slot horizontally-aligned switch. The Catalyst 6503 switch supports the following:

- A supervisor engine with two gigabit interface uplinks and an optional redundant supervisor engine in one of the following configurations:
  - Two supervisor engines, each with no Multilayer Switch Feature Card (MSFC) and no Policy Feature Card (PFC)
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card

  Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

  Note Both supervisor engines in a single chassis must be completely identical.

- Up to two hot-swappable Catalyst 6500 series modules:
  - The Switch Fabric Modules (WS-C6500-SFM and WS-X6500-SFM2) are not supported on the Catalyst 6503 switch.
  - The WS-X6816-GBIC 16-port Gigabit Ethernet fabric-enabled module is not supported on the Catalyst 6503 switch.
- Backplane bandwidth of 32 Gbps
- Hot-swappable fan assembly
- Two power entry modules (PEMs)
- Redundant AC-input or DC-input power supplies (950W power supply only)

Figure 1-1 Catalyst 6503 Switch—Front View

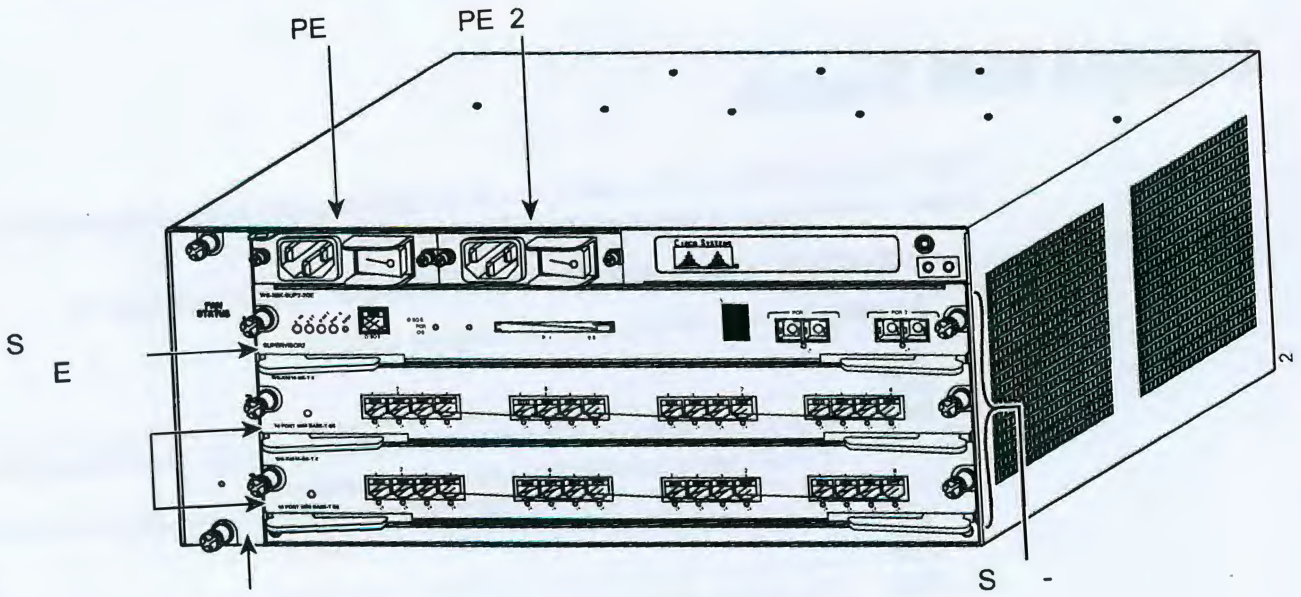
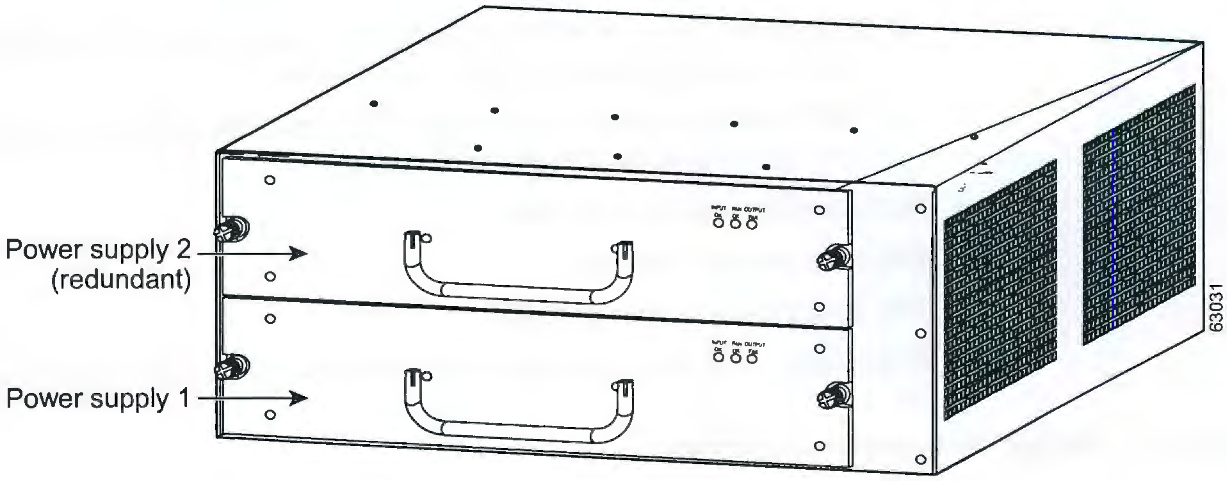


Figure 1-2 Catalyst 6503 Switch—Rear View



Catalyst 6506 Switch

The Catalyst 6506 switch chassis is a 6-slot horizontally-aligned chassis. The Catalyst 6506 switch supports the following:

- A supervisor engine with two Gigabit Ethernet uplink ports (slot 1)
- An optional redundant supervisor engine (slot 2)

Note Supervisor Engine 720 must be installed in chassis slots 5 or 6. Slots 1 and 2 are available for switching modules.

Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6506 switch in one of three configurations:

  - Two supervisor engines, each with no Multilayer Switch Feature Card (MSFC) and no Policy Feature Card (PFC)
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Up to five additional hot-swappable Catalyst 6500 series switching modules
  - Fabric-enabled module support provided in slots 2–6 (requires Switch Fabric Module)

    Note Supervisor Engine 720 has built-in switching fabric and does not require that Switch Fabric Modules be installed in the chassis.

- Hot-swappable fan tray

  Note The high capacity fan tray (WS-C6K-6SLOT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

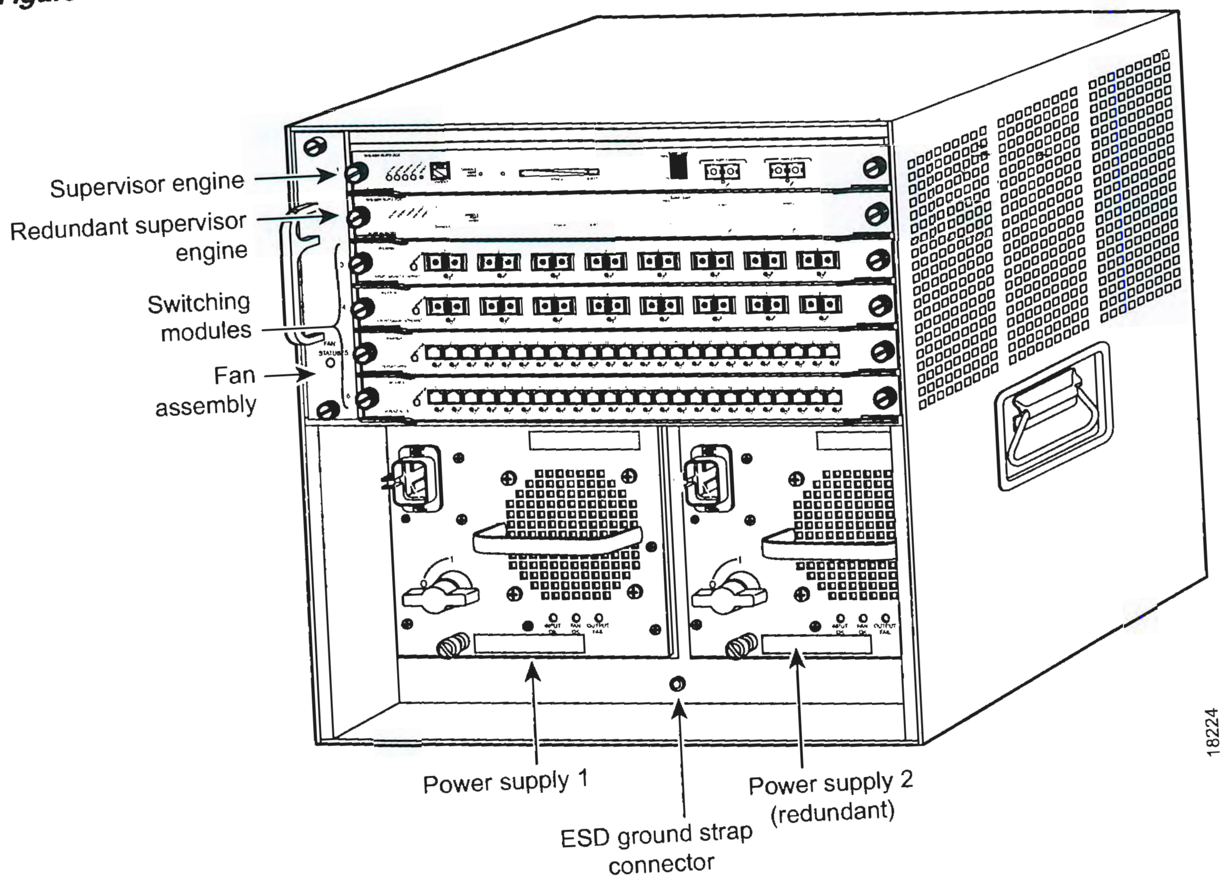
- Redundant AC-input or DC-input power supplies

  Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

- Backplane bandwidth of 32 Gbps scalable up to 256 Gbps

  Note Backplane bandwidth greater than 32 Gbps requires that you install either a Switch Fabric Module or a Supervisor Engine 720 in the switch chassis.

Figure 1-3 Catalyst 6506 Switch


Supervisor engine
Redundant supervisor engine
Switching modules
Fan assembly
Power supply 1
ESD ground strap connector
Power supply 2 (redundant)
18224

A

- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - The Switch Fabric Module requires Supervisor Engine 2.

    Note Switch Fabric Modules are not supported by Supervisor Engine 720.

  - You must install a Switch Fabric Module in either slot 5 or slot 6 of the Catalyst 6506 switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 acts as the primary module, and the module in slot 6 acts as the backup. If you reset the module in slot 5, the module in slot 6 becomes the primary module.
  - Mixing an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis is supported.
  - Fabric-enabled module support is provided in all slots. (A Switch Fabric Module is required.)

Catalyst 6509 Switch

The Catalyst 6509 switch chassis has nine horizontal slots that are numbered from top to bottom. (See Figure 1-4.) Slot 1 is reserved for the supervisor engine, which provides switching, local and remote management, and multiple gigabit uplink interfaces.

Slot 2 can contain an additional supervisor engine, which can act as a backup if the first supervisor engine fails. If a redundant supervisor engine is not required, slot 2 is available for a switching module.

For a detailed description of supervisor engine operation in a redundant configuration, refer to your software configuration guide.

The Catalyst 6509 switch supports the following:

- A supervisor engine with two Gigabit Ethernet uplink ports and an optional redundant supervisor engine

  Note Supervisor Engine 720 must be installed in chassis slots 5 or 6. Slots 1 and 2 are available for switching modules.

  Note The uplink ports are fully functional on a redundant supervisor engine in standby mode.

  Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6500 series switch in one of three configurations:

  - Two supervisor engines, each with no MSFC and no PFC
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Backplane bandwidth scalable up to 256 Gbps

  Note Backplane bandwidth greater than 32 Gbps requires that you install a Switch Fabric Module or a Supervisor Engine 720 in the Catalyst 6509-NEB switch chassis.

- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - The Switch Fabric Modules require Supervisor Engine 2.
  - You must install the Switch Fabric Module in either slot 5 or slot 6 of the Catalyst 6509-NEB switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 acts as the primary module, and the module in slot 6 acts as the backup. If you reset the module in slot 5, the module in slot 6 becomes the primary module.

  - Mixing an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis is supported.

    Note Supervisor Engine 720 has built-in switching fabric and does not require that Switch Fabric Modules be installed in the chassis.

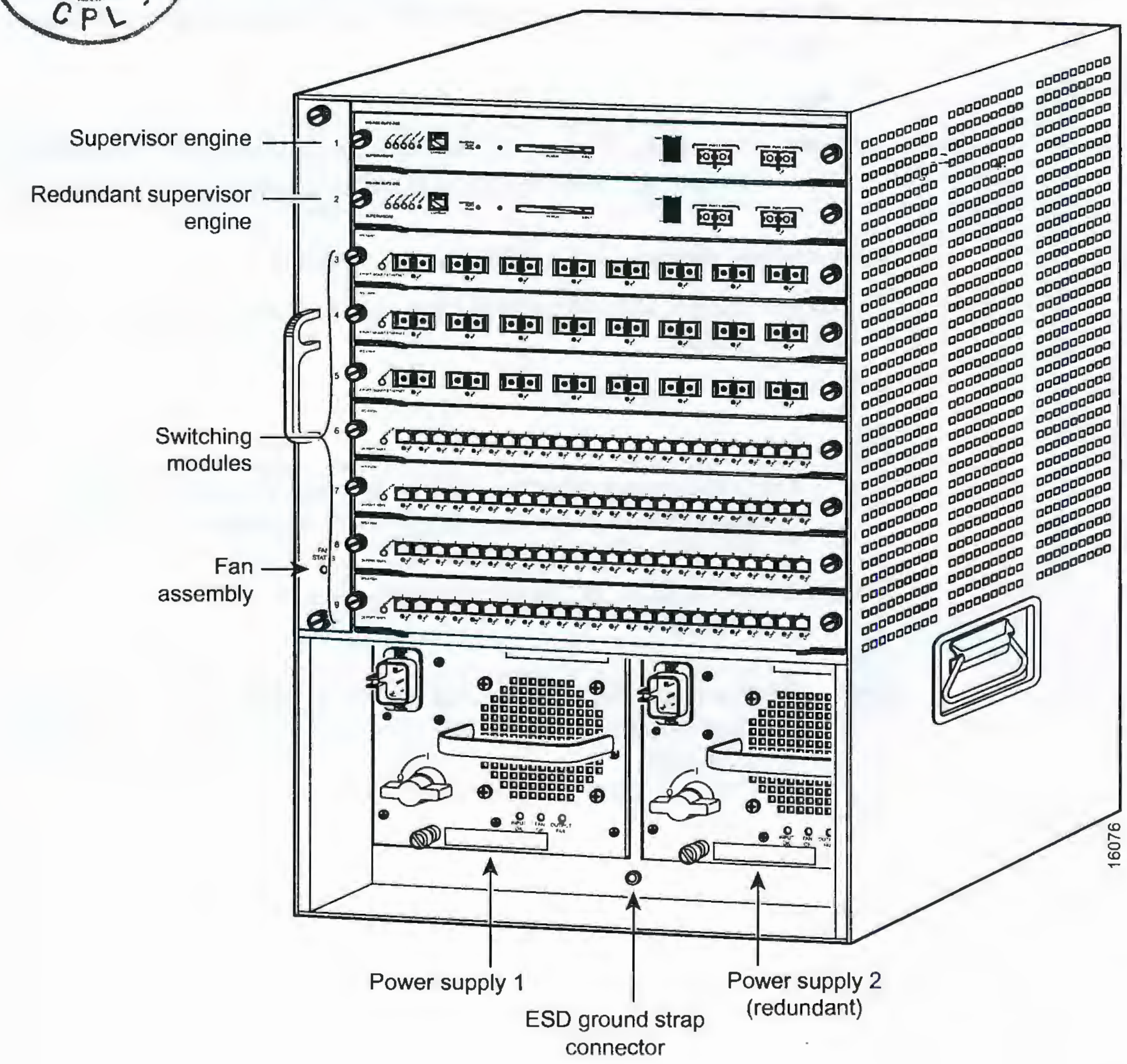
- Up to eight additional Catalyst 6500 series modules
  - Fabric-enabled module support provided in all slots (requires Switch Fabric Module)
- Hot-swappable fan assembly

  Note The high capacity fan tray (WS-C6K-9SLOT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

- Redundant AC-input or DC-input power supplies

  Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

Figure 1-4 Catalyst 6509 Switch


Supervisor engine
Redundant supervisor engine
Switching modules
Fan assembly
Power supply 1
ESD ground strap connector
Power supply 2 (redundant)
16076

Catalyst 6509-NEB Switch

The Catalyst 6509-NEB switch chassis has nine vertical slots that are numbered from right to left. (See Figure 1-5.) Slot 1 is reserved for the supervisor engine, which provides switching, local and remote management, and multiple gigabit uplink interfaces.

Slot 2 can contain an additional supervisor engine, which can act as a backup if the first supervisor engine fails. If a redundant supervisor engine is not required, slot 2 is available for a switching module.

For a detailed description of supervisor engine operation in a redundant configuration, refer to your software configuration guide.

The Catalyst 6509-NEB switch supports the following:

- A supervisor engine with two Gigabit Ethernet uplink ports and an optional redundant supervisor engine

Note Supervisor Engine 720 must be installed in slots 5 or 6. Slots 1 and 2 are available for switching modules.

Note The uplink ports are fully functional on the redundant supervisor engine in standby mode.

Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6500 series switch in one of three configurations:

  - Two supervisor engines, each with no MSFC and no PFC
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Backplane bandwidth scalable up to 256 Gbps

Note Backplane bandwidth greater than 32 Gbps requires that you install either a Switch Fabric Module or a Supervisor Engine 720 in the Catalyst 6509-NEB switch chassis.

- A Switch Fabric Module (WS-C6500-SFM or WS-X6500-SFM2)
  - The Switch Fabric Modules require Supervisor Engine 2.
  - You must install the Switch Fabric Module in either slot 5 or slot 6 of the Catalyst 6509-NEB switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 5 acts as the primary module, and the module in slot 6 acts as the backup. If you reset the module in slot 5, the module in slot 6 becomes the primary module.
  - Mixing an SFM (WS-C6500-SFM) with an SFM2 (WS-X6500-SFM2) in the same Catalyst 6506, Catalyst 6509, or Catalyst 6509-NEB chassis is supported.

    Note The Supervisor Engine has built-in switching fabric and does not require that Switch Fabric Modules be installed in the chassis.

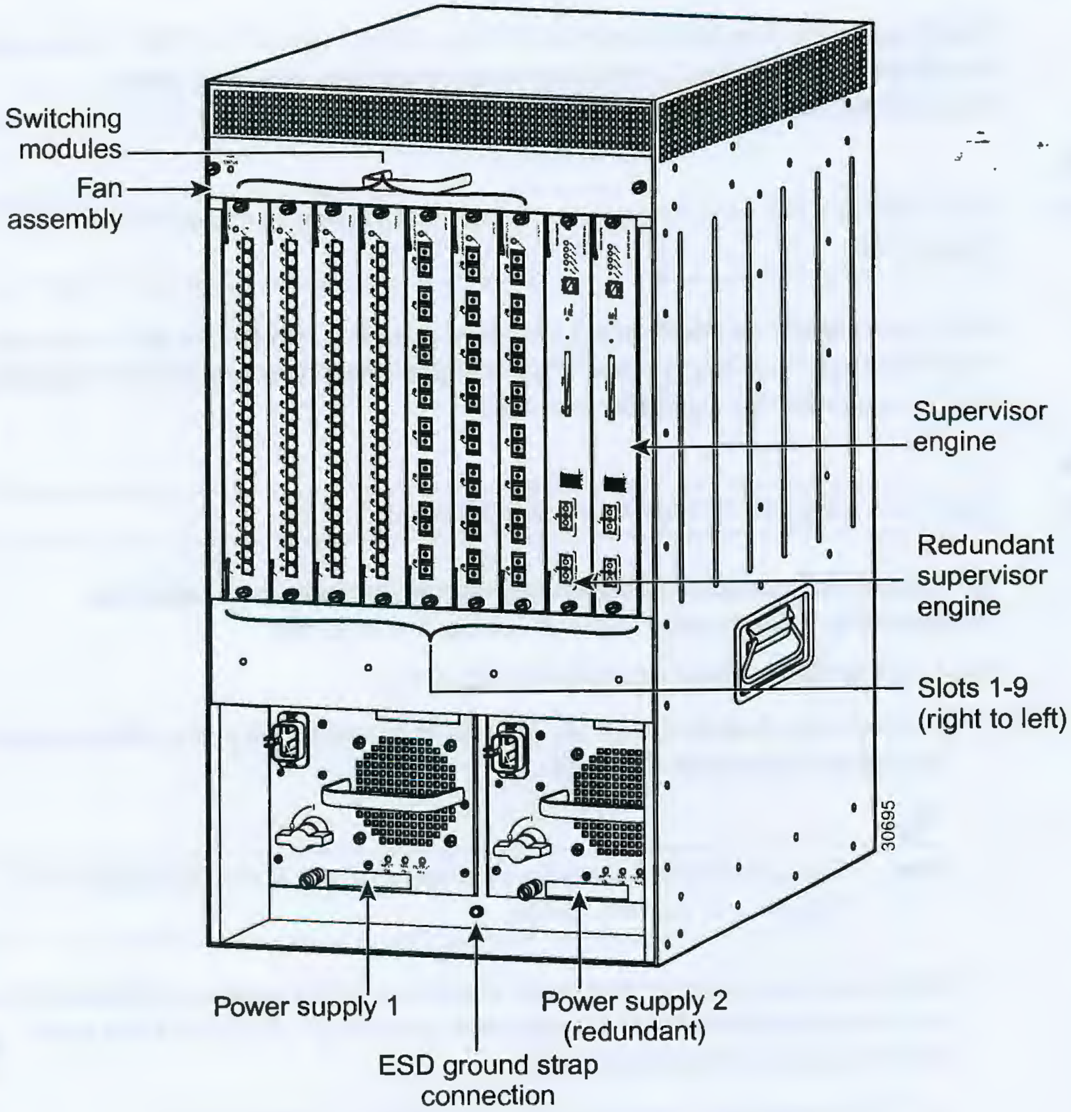
- Up to eight additional Catalyst 6500 series hot-swappable modules
  - Fabric-enabled module support provided in all slots (requires Switch Fabric Module or Supervisor Engine 720)
- Hot-swappable fan assembly

Note The high capacity fan tray (WS-C6509-NEB-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

- Redundant AC-input or DC-input power supplies

Note When a Supervisor Engine 720 and the high capacity fan tray are installed, you must install 2500 W or larger capacity power supplies in the chassis.

Figure 1-5 Catalyst 6509-NEB Switch


Switching modules
Fan assembly
Supervisor engine
Redundant supervisor engine
Slots 1-9 (right to left)
30695
Power supply 1
ESD ground strap connection
Power supply 2 (redundant)

Catalyst 6513 Switch

The Catalyst 6513 switch chassis has 13 slots. (See Figure 1-6.) Slot 1 is reserved for a Supervisor Engine 2, which provides switching, local and remote management, and multiple gigabit uplink interfaces.

Note The Catalyst 6513 switch requires a Supervisor Engine 2 or Supervisor Engine 720.

Slot 2 can contain an additional Supervisor Engine 2, which can act as a backup if the first supervisor engine fails. If a redundant supervisor engine is not required, slot 2 is available for a switching module.

Note Supervisor Engine 720 must be installed in slots 7 or 8.

For a detailed description of supervisor engine operation in a redundant configuration, refer to your software configuration guide

The Catalyst 6513 switch supports the following:

- A Supervisor Engine 2 with two Gigabit Ethernet uplink ports and an optional redundant Supervisor Engine 2

  Note The uplink ports are fully functional on the redundant Supervisor Engine 2 in standby mode.

  Both supervisor engines in a single chassis must be completely identical. You can configure the redundant supervisor engines in a Catalyst 6500 series switch in one of three configurations:

  - Two supervisor engines, each with no MSFC and no PFC
  - Two supervisor engines, each configured with a PFC daughter card
  - Two supervisor engines, each configured with both an MSFC and a PFC daughter card

- Backplane bandwidth scalable up to 256 Gbps

Note Backplane bandwidth greater than 32 Gbps requires that you install either a Switch Fabric Module or Supervisor Engine 720 in the Catalyst 6513 switch chassis.

- A Switch Fabric Module (supports WS-X6500-SFM2 only)
  - The Switch Fabric Module requires Supervisor Engine 2. Supervisor Engine 1A does not support the Switch Fabric Module.
  - You must install the Switch Fabric Module in slot 7 or slot 8 of the Catalyst 6513 switch. For redundancy, you can install a standby Switch Fabric Module. The module first installed functions as the primary module. When you install two Switch Fabric Modules at the same time, the module in slot 7 acts as the primary module, and the module in slot 8 acts as the backup. If you reset the module in slot 7, the module in slot 8 becomes the primary module.

    Note Supervisor Engine 720 has built-in switching fabric and does not require that Switching Fabric Modules be installed in the chassis.

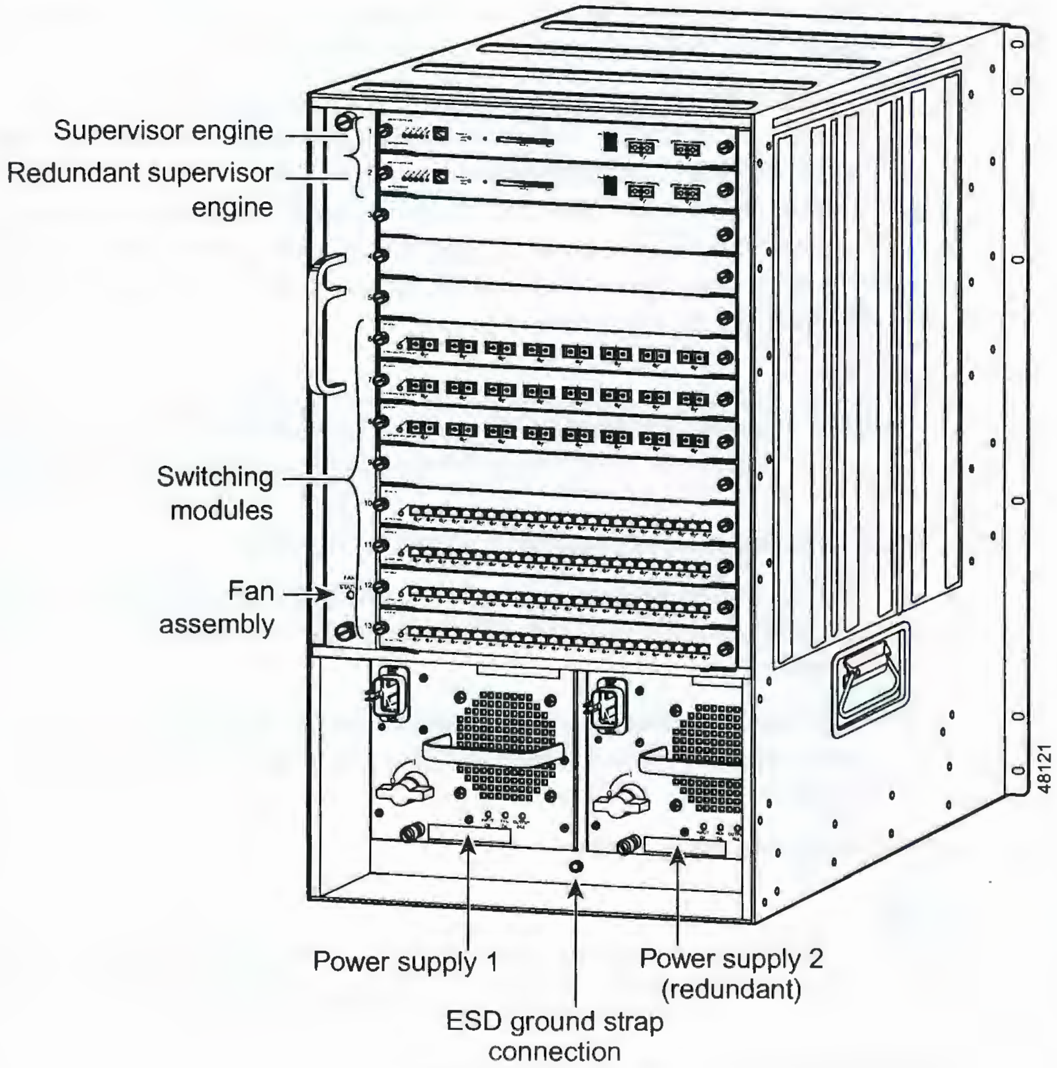
- Up to 12 additional hot-swappable switching modules
  - Fabric-enabled module support provided in all slots (requires a Switch Fabric Module (WS-X6500-SFM2) or Supervisor Engine 720 be installed)
  - Dual Fabric connectivity supported in slots 9–13 (requires a Switch Fabric Module (WS-X6500-SFM2) or Supervisor Engine 720 be installed)
- Hot-swappable fan assembly

  Note The high capacity fan tray (WS-C6K-13SLT-FAN2) must be installed when a Supervisor Engine 720 is installed in the chassis.

- Redundant AC-input or DC-input power supplies

Note When a Supervisor Engine 720 and the higher capacity fan tray are installed, you must install 2500 W or higher capacity power supplies in the chassis.

Figure 1-6 Catalyst 6513 Switch


Supervisor engine
Redundant supervisor engine
Switching modules
Fan assembly
Power supply 1
ESD ground strap connection
Power supply 2 (redundant)
48121

System Features

This section describes the hardware features for the Catalyst 6500 series switches. For software descriptions, refer to your software configuration guide. For module descriptions and installation procedures, refer to the *Catalyst 6500 Series Switches Module Installation Guide*.

Port Density

Table 1-2 lists the port densities of the Catalyst 6500 series switches.

Table 1-2 Catalyst 6500 Series Port Density

Architecture	Catalyst 6500 Series Switches
Number of 10 Gigabit Ethernet Ports	2 (3 slots) Catalyst 6503 switch 5 (6 slots) Catalyst 6506 switch 8 (9 slots) Catalyst 6509 switch 12 (13 slots) Catalyst 6513 switch
Number of Gigabit Ethernet Ports	34 (3 slots) Catalyst 6503 switch 82 (6 slots) Catalyst 6506 switch 130 (9 slots) Catalyst 6509 switch 194 (13 slots) Catalyst 6513 switch
Number of 100BASE-FX Ethernet Ports	96 (3 slots) Catalyst 6503 switch 120 (6 slots) Catalyst 6506 switch 192 (9 slots) Catalyst 6509 switch 288 (13 slots) Catalyst 6513 switch
Number of 10/100 Ethernet Ports	96 (3 slots) Catalyst 6503 switch 240 (6 slots) Catalyst 6506 switch 384 (9 slots) Catalyst 6509 switch 576 (13 slots) Catalyst 6513 switch
Number of 10BASE-FL Ethernet Ports	48 (3 slots) Catalyst 6503 switch 120 (6 slots) Catalyst 6506 switch 192 (9 slots) Catalyst 6509 switch 288 (13 slots) Catalyst 6513 switch

Table 1-2 Catalyst 6500 Series Port Density (continued)

Architecture	Catalyst 6500 Series Switches
Number of ATM OC-12 Ports	2 (3 slots) Catalyst 6503 switch 5 (6 slots) Catalyst 6506 switch 8 (9 slots) Catalyst 6509 switch 12 (13 slots) Catalyst 6513 switch
Number of FlexWAN Modules	2 (3 slots) Catalyst 6503 switch 5 (6 slots) Catalyst 6506 switch 8 (9 slots) Catalyst 6509 switch 12 (13 slots) Catalyst 6513 switch

Redundancy

Catalyst 6500 series switches have these redundancy features:

- Ability to house two hot-swappable supervisor engines
- Ability to house two fully redundant, AC-input or DC-input, load-sharing power supplies

Note In certain configurations, the power supplies are not fully redundant. Refer to the "Power Supply Redundancy" section on page 1-29.

- A hot-swappable fan assembly containing multiple fans
- Redundant backplane-mounted clock modules
- Redundant backplane-mounted voltage termination (VTT) modules

Component Hot Swapping

You can hot swap all modules (including the supervisor engine if you have a redundant supervisor engine) and the fan assembly. You can add, replace, or remove modules without interrupting the system power or causing other software or interfaces to shut down.

Fan Assembly

The system fan assembly is located in the chassis and provides cooling air for the supervisor engine and the switching modules. The following figures show the direction of airflow into and out of the switch: Figure 1-7 (Catalyst 6503 switch), Figure 1-8 (Catalyst 6506 switch), Figure 1-9 (Catalyst 6509 switch), Figure 1-10 (Catalyst 6509-NEB switch), and Figure 1-11 (Catalyst 6513 switch). Sensors on the supervisor engine monitor the internal air temperatures. If the air temperature exceeds a preset threshold, the environmental monitor displays warning messages.

Note We recommend that you maintain a minimum air space of 6 inches (15 cm) between walls and the chassis air vents and a minimum horizontal separation of 12 inches (30.5 cm) between two chassis to prevent overheating.

If an individual fan within the assembly fails, the FAN STATUS LED turns red. Individual fans cannot be replaced. To replace a fan assembly, see the "Removing and Replacing the Fan Assembly" section on page 5-35.

Refer to your software configuration guide for information on environmental monitoring.

Figure 1-7 Catalyst 6503 Switch Internal Airflow

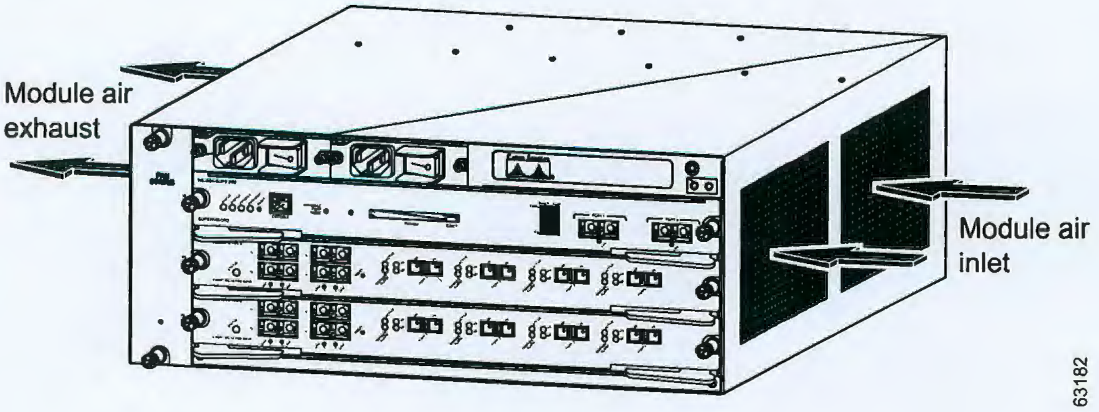


Figure 1-8 Catalyst 6506 Switch Internal Airflow

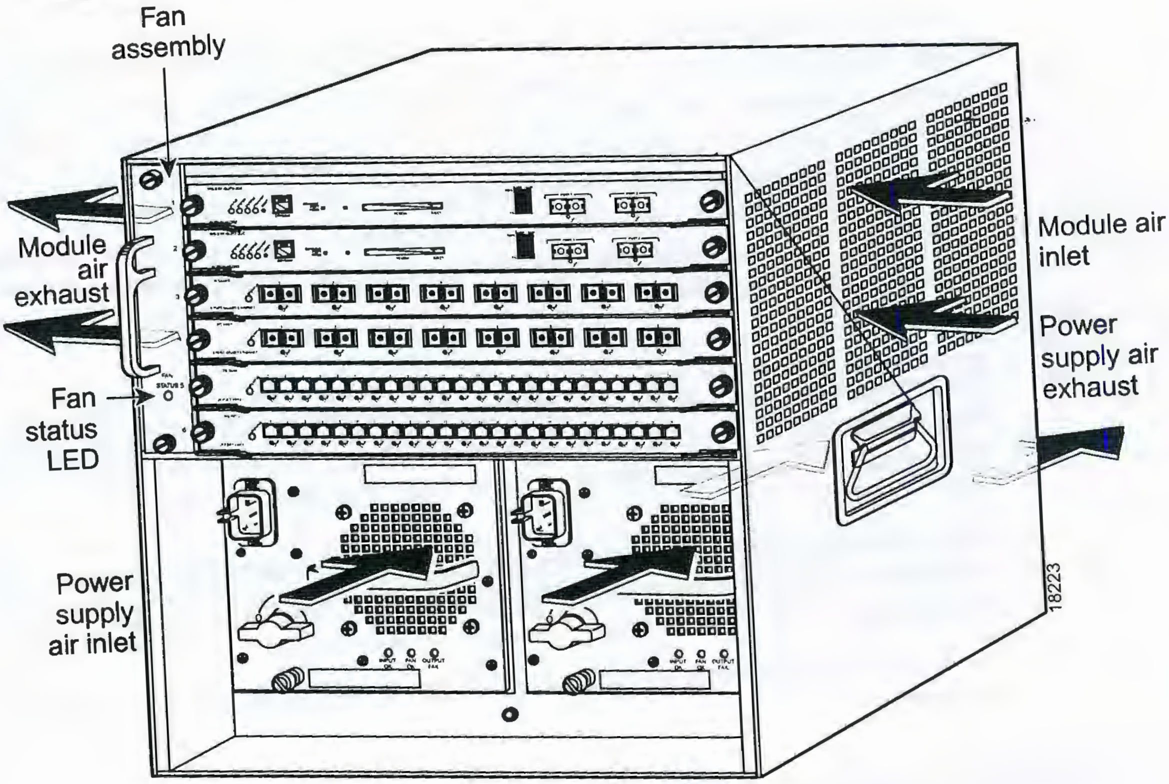


Figure 1-9 Catalyst 6509 Switch Internal Airflow

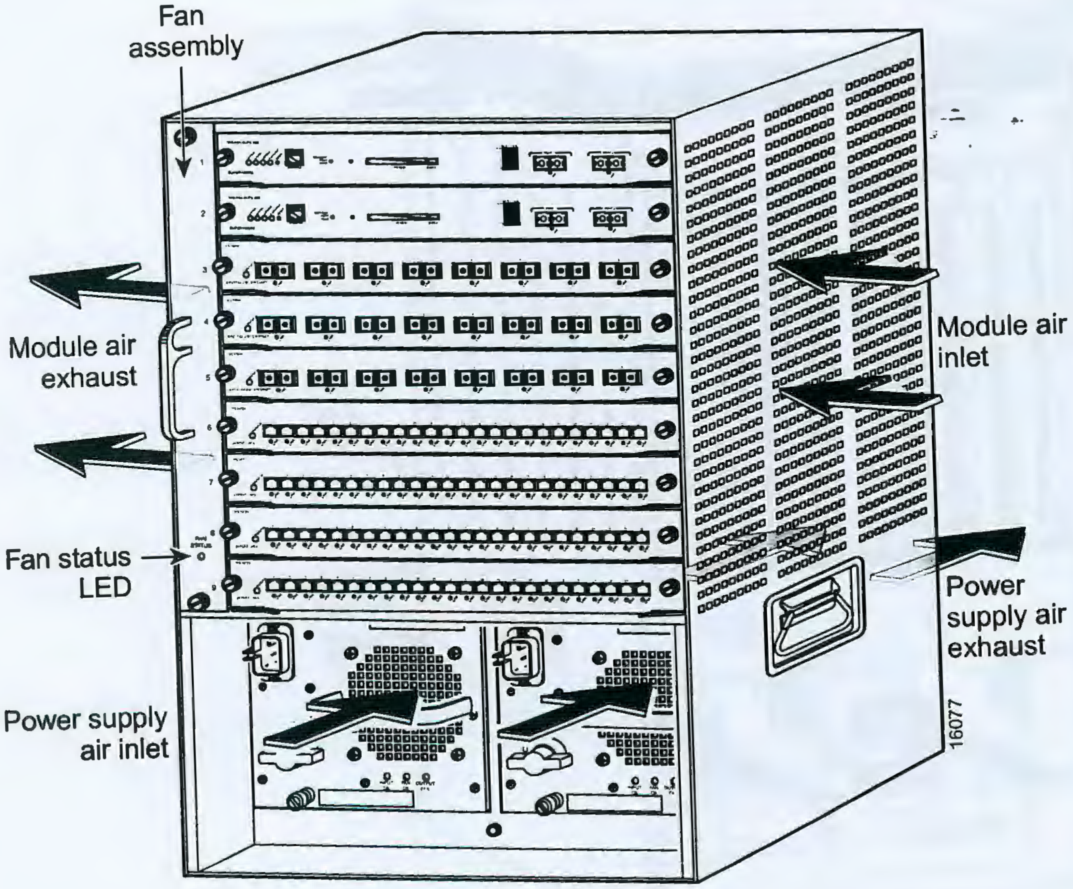


Figure 1-10 Catalyst 6509-NEB Switch Internal Airflow

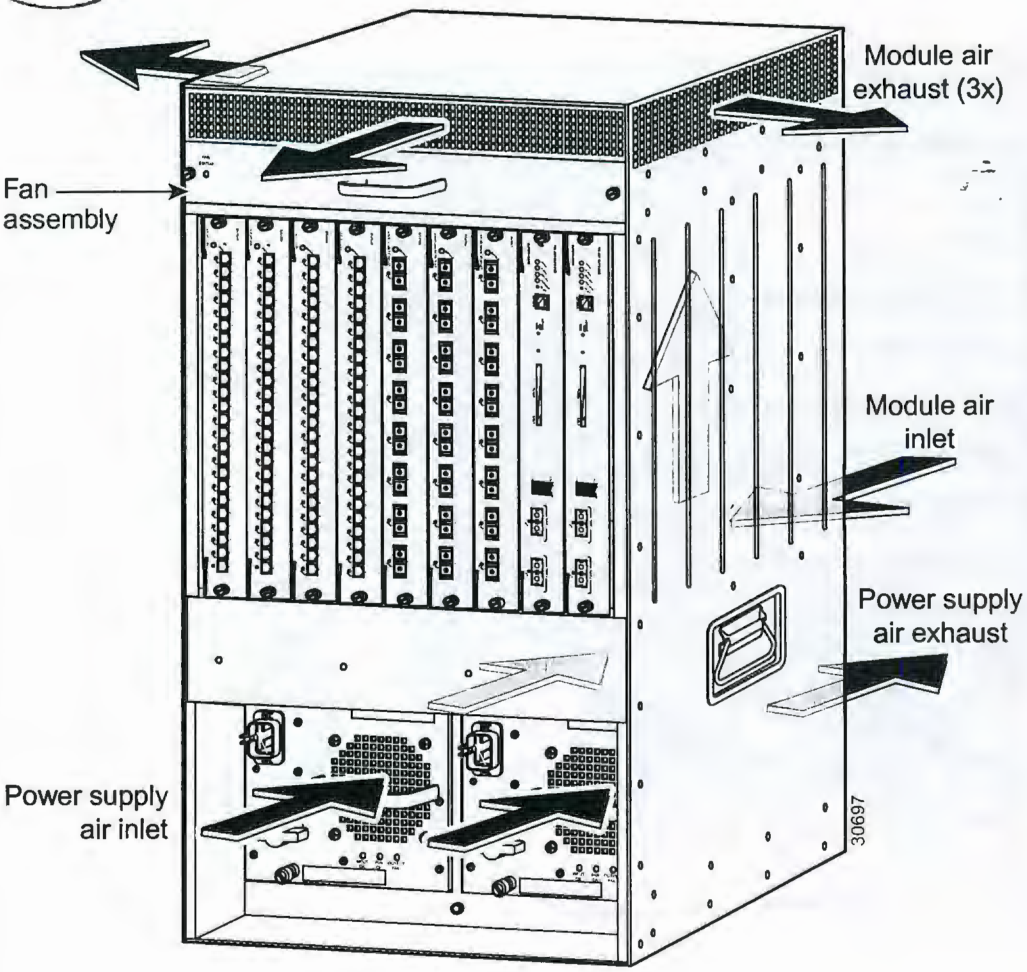
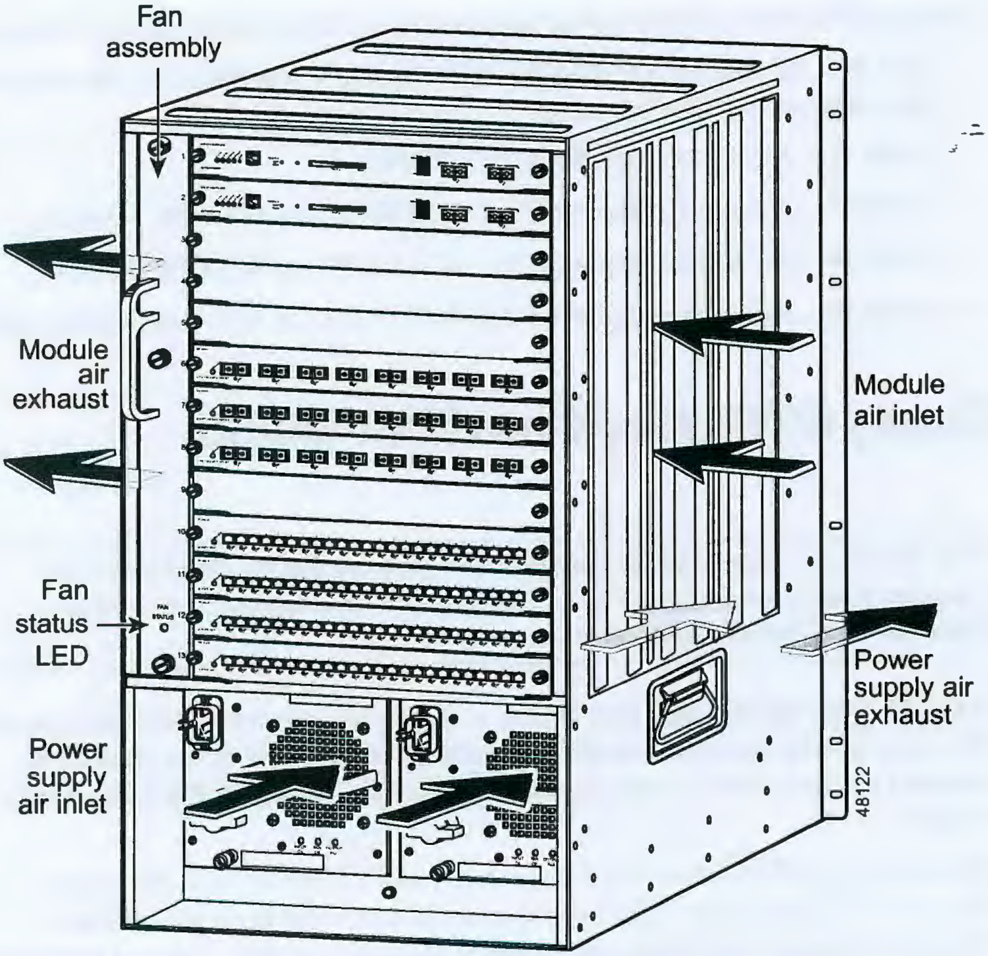


Figure 1-11 Catalyst 6513 Switch Internal Airflow



Power Supplies

Catalyst 6500 series switch power supplies are available in five power ratings:

- 950 W—AC and DC input (PWR-950-AC and PWR-950-DC) (for use with the Catalyst 6503 switch only)
- 1000 W—AC input only (WS-CAC-1000W)
- 1300 W—AC and DC input (WS-CAC-1300W and WS-CDC-1300W)
- 2500 W—AC and DC input (WS-CAC-2500W and WS-CDC-2500W)
- 4000 W—AC input only (WS-CAC-4000W-US1 or WS-CAC-4000W-INT)

950 W Power Supply (PWR-950-AC and PWR-950-DC)

Note The 950 W AC-input and DC-input power supplies can be installed in the Catalyst 6503 switch chassis only. They cannot be installed in any other Catalyst 6500 series switch chassis.

The 950 W power supplies (see Figure 1-12) do not connect directly to source AC but use a power entry module (PEM), located on the front of the chassis, to connect the site power source to the power supply located in the back of the chassis.

The AC-input PEM (shown in Figure 1-13) and DC-input PEM (shown in Figure 1-14) provide an input power connection on the front of the router chassis to connect the site power source to the power supply. You can connect the DC-input power supply to the power source with heavy gauge wiring connected to a terminal block. The wire gauge size is determined by local electrical codes and restrictions.

Note The power cord is not shown in Figure 1-13.

The PEMs have an illuminated power switch (AC-input only), current protection, surge and EMI suppression, and filtering functions.

Figure 1-12 Catalyst 6503 950 W AC- and DC-Input Power Supplies

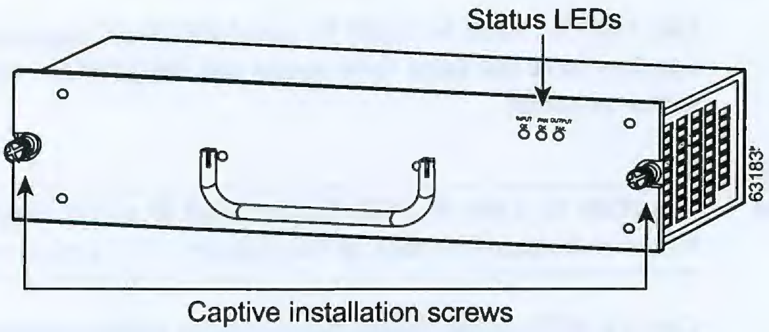


Figure 1-13 Catalyst 6503 AC Power Entry Module (PEM)

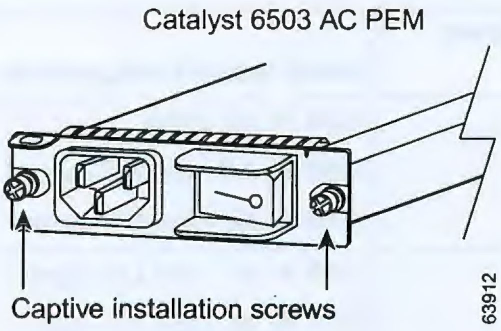
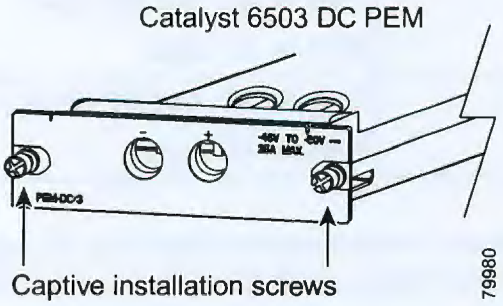


Figure 1-14 Catalyst 6503 DC Power Entry Module (PEM)



1000 W, 1300 W, 2500 W, and 4000 W Power Supplies

The 1000 W, 1300 W, 2500 W, and 4000 W AC-input and DC-input power supplies have the same form factor and designed for use in the Catalyst 6500 series switches.

Note The 1000 W, 1300 W, 2500 W, and 4000 W power supplies have a different form factor and cannot be used in the Catalyst 6503 series switch.

Catalyst 6500 series chassis power supply configurations for the 1000 W, 1300 W, 2500 W and 4000 W power supplies are shown in Table 1-3.

Table 1-3 Catalyst 6500 Series Power Supply Configurations

Catalyst 6500 Series Switch	Power Supply Configurations
Catalyst 6506	1000 W AC-input 1300 W AC- and DC-input 2500 W AC- and DC-input
Catalyst 6509	1300 W AC- and DC-input 2500 W AC- and DC-input 4000 W AC-input
Catalyst 6509-NEB	1300 W AC- and DC-input 2500 W AC- and DC-input 4000 W AC-input
Catalyst 6513	2500 W AC- and DC-input 4000 W AC-input

Catalyst 6500 series switches support redundant AC-input and DC-input power supplies. Unlike the Catalyst 4000 family and Catalyst 5000 family switches, the Catalyst 6500 series switches allow you to mix AC-input and DC-input power supplies in the same chassis.

Many telco organizations require a –48 VDC power supply to accommodate their power distribution systems. From an operational perspective, the DC-input power supply has the same characteristics as the AC-input version.

The AC-input power supply (see Figure 1-15) has a detachable power cord (except for the WS-CAC-4000W) that allows you to connect each power supply to the site power source. You can connect the DC-input power supply (see Figure 1-16) to the power source with heavy gauge wiring connected to a terminal block. The wire gauge size is determined by local electrical codes and restrictions.

Note The power cord is not shown in Figure 1-15.

Note With a fully populated Catalyst 6513 switch, two 2500 W power supplies are not fully redundant. If you run the 2500 W power supply at the low range input (100 to 120 VAC), it is not redundant in a fully populated Catalyst 6509 or Catalyst 6509-NEB switch.

Note The 2500 W AC-input power supply needs 220 VAC to deliver 2500 W of power. When powered with 110 VAC, it delivers only 1300 W. In addition, the power supply needs 16 A, regardless of whether it is plugged into 110 VAC or 220 VAC.

For complete power specifications, see Appendix A, "Technical Specifications."

Figure 1-15 AC-Input Power Supply

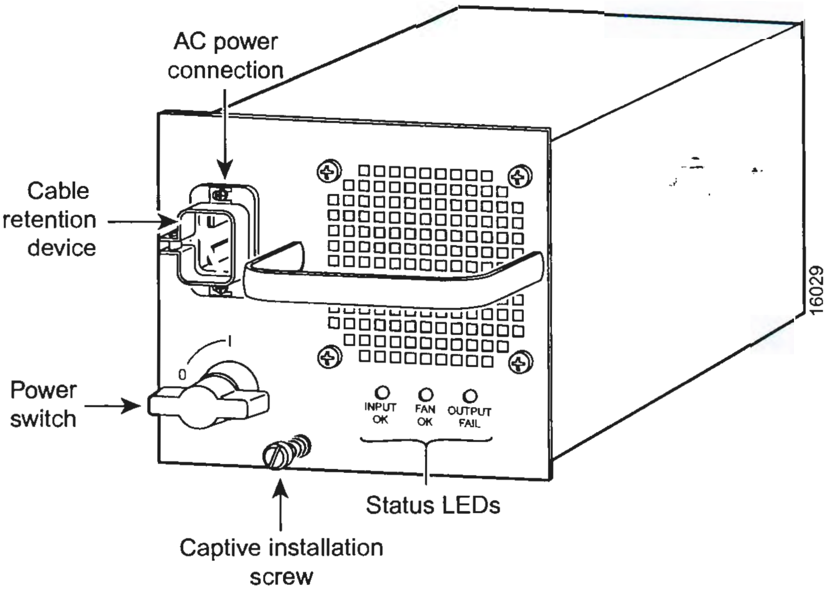
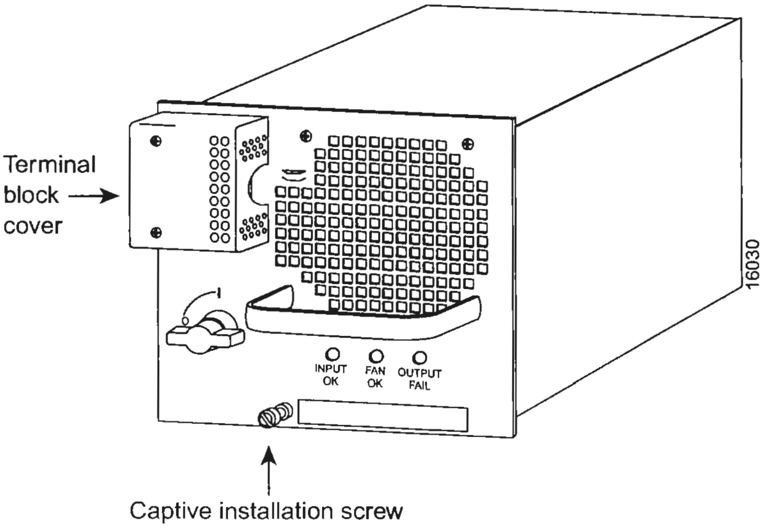


Figure 1-16 DC-Input Power Supply



Power Supply Redundancy

Catalyst 6500 series modules have different power requirements. Depending upon the wattage of the power supply, certain switch configurations might require more power than a single power supply can provide. Although the power management feature allows you to power all installed modules with two power supplies, redundancy is not supported in this configuration. Redundant and nonredundant power configurations are summarized in Table 1-4. The effects of changing the power supply configurations are summarized in Table 1-5.

Note For proper load-sharing operation in a redundant power supply configuration, you must install two modules in the chassis. If you fail to install two modules, you might receive spurious OUTPUT FAIL indications on the power supply.

Table 1-4 Power Supply Redundancy

If you have two power supplies of	and redundancy is	Then
Equal wattage	Enabled	The total power drawn from both supplies is never greater than the capability of one supply. If one supply malfunctions, the other supply can take over the entire system load. Each power supply provides approximately half of the required power to the system. Load sharing and redundancy are enabled automatically; no software configuration is required.
Unequal wattage	Enabled	Both power supplies come online, but a syslog message displays that the lower wattage power supply will be disabled. If the active power supply fails, the system shuts down. The lower wattage power supply must then be manually turned on. The lower wattage power supply selectively powers up the modules so that the capacity of the power supply is not exceeded.
Equal or unequal wattage	Disabled	The total power available to the system is approximately 167 percent of the lower wattage power supply. The system powers up as many modules as the combined capacity allows. If the higher wattage power supply fails, the lower wattage supply might also shut down due to overcurrent protection, thus preventing damage to the lower wattage power supply.

Table 1-5 Effects of Power Supply Configuration Changes

Configuration Change	Effect
Redundant to nonredundant	• System log and syslog messages are generated. • System power is increased to approximately 167 percent of the lower wattage power supply. • The modules marked as *power-deny* in the **show module** Status field are brought up if there is sufficient power.
Nonredundant to redundant	• System log and syslog messages are generated. • System power is the power capability of the larger wattage supply. • If there is not enough power for all previously powered-up modules, some modules are powered down and marked as *power-deny* in the **show module** Status field.
Equal wattage power supply is inserted with redundancy enabled	• System log and syslog messages are generated. • System power equals the power capability of one supply (both supplies provide approximately one half of the total current). • No change in the module status because the power capability is unchanged.
Equal wattage power supply is inserted with redundancy disabled	• System log and syslog messages are generated. • System power is the combined power capability of both supplies. • The modules marked as *power-deny* in the **show module** Status field are brought up if there is sufficient power.
Higher wattage power supply is inserted with redundancy enabled	• System log and syslog messages are generated. • The system disables the lower wattage power supply; the higher wattage supply powers the system.
Lower wattage power supply is inserted with redundancy enabled	• System log and syslog messages are generated. • The system disables the lower wattage power supply; the higher wattage supply powers the system.

Table 1-5 Effects of Power Supply Configuration Changes (continued)

Higher or lower wattage power supply is inserted with redundancy disabled	• System log and syslog messages are generated. • System power is increased to the combined power capability of both supplies. • The modules marked as *power-deny* in the **show module** Status field are brought up if there is sufficient power.
Power supply is removed with redundancy enabled	• System log and syslog messages are generated. • If the power supplies are of equal wattage, there is no change in the module status because the power capability is unchanged. If the power supplies are of unequal wattage and the lower wattage supply is removed, there is no change in the module status. If the power supplies are of unequal wattage and the higher wattage supply is removed, the lower wattage power supply must be manually turned on. (The system had previously turned off the lower wattage power supply.)
Power supply is removed with redundancy disabled	• System log and syslog messages are generated. • System power is decreased to the power capability of one supply. • If there is not enough power for all previously powered-up modules, some modules are powered down and marked as *power-deny* in the **show module** Status field.
System is booted with power supplies of different wattage installed and redundancy enabled	• System log and syslog messages are generated. • The lower wattage supply is disabled.
System is booted with power supplies of equal or different wattage installed and redundancy disabled	• System log and syslog messages are generated. • System power equals the combined power capability of both supplies. • The system powers up as many modules as the combined capacity allows.

You can change the configuration of the power supplies to redundant or nonredundant at any time. If you switch from a redundant to a nonredundant configuration, both power supplies are enabled (even a power supply that was disabled because it was of a lower wattage than the other power supply). If you change from a nonredundant to a redundant configuration, both power supplies are initially enabled, and if they are of the same wattage, remain enabled. If they are of different wattage, a syslog message displays and the lower wattage supply is disabled.

For additional information about the power management feature and individual module power consumption, refer to your software configuration guide.

Environmental Monitoring of the Power Supply

The environmental monitoring and reporting functions allow you to maintain normal system operation by resolving adverse environmental conditions prior to loss of operation.

The power supplies monitor their own internal temperature and voltages. In the event of excessive internal temperature, the power supply will shut down to prevent damage. When the power supply returns to a safe operating temperature, it will restart. In the event of an abnormal voltage on one or more outputs of the power supplies, the OUTPUT FAIL LED will light. Substantial overvoltage conditions can lead to a power supply shutdown.

The power supply front panel LEDs are described in Table 1-6.

For more information about the environmental monitoring feature, refer to your software configuration guide.

Table 1-6 Power Supply Front Panel LEDs

LED	Description
INPUT OK	AC-input power supplies: • Green when the input voltage is OK (85 VAC or greater) • Off when the input voltage falls below 70 VAC or if the power supply shuts down DC-input power supplies: • Green when the input voltage is OK (–40.5 VDC or greater) • Off when the input voltage falls below –33 VDC or if the power supply shuts down
FAN OK	Green when the power supply fan is operating properly. Red when a power supply fan failure is detected.
OUTPUT FAIL	Red when there is a problem with one or more of the DC-output voltages of the power supply

Power Supply Fan Assembly

The power supplies have a built-in fan; air enters the front of the fan (power-input end) and exits through the back. An air dam keeps the airflow separate from the rest of the chassis, which is cooled by the system fan assembly.

Power supply fans are not field-replaceable; the power supply must be replaced. To replace a power supply, see the "Removing and Replacing the 1000 W, 1300 W, 2500 W, and 4000 W Power Supplies" section on page 5-20.

Apêndice FI

CHAPTER 9

Configuring VLANs

This chapter describes how to configure VLANs on the Catalyst 6500 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

This chapter consists of these sections:

- Understanding How VLANs Work, pagc 9-1
- VLAN Default Configuration, page 9-6
- VLAN Configuration Guidelines and Restrictions, page 9-8
- Configuring VLANs, page 9-8

Understanding How VLANs Work

The following sections describe how VLANs work:

- VLAN Overview, page 9-1
- VLAN Ranges, page 9-2
- Configurable VLAN Parameters, pagc 9-3
- Understanding Token Ring VLANs, page 9-3

VLAN Overview

A VLAN is a group of end stations with a common set of requirements, independent of physical location. VLANs have the same attributes as a physical LAN but allow you to group end stations even if they are not located physically on the same LAN segment.

VLANs are usually associated with IP subnetworks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. LAN port VLAN membership is assigned manually on an port-by-port basis.

VLAN Ranges

Note You must enable the extended system ID to use 4096 VLANs (see the "Understanding the Bridge ID" section on page 15-3).

With Release 12.1(13)E and later releases, Catalyst 6500 series switches support 4096 VLANs in accordance with the IEEE 802.1Q standard. These VLANs are organized into several ranges; you use each range slightly differently. Some of these VLANs are propagated to other switches in the network when you use the VLAN Trunking Protocol (VTP). The extended-range VLANs are not propagated, so you must configure extended-range VLANs manually on each network device.

Table 9-1 describes the VLAN ranges.

Table 9-1 VLAN Ranges

VLANs	Range	Usage	Propagated by VTP
0, 4095	Reserved	For system use only. You cannot see or use these VLANs.	—
1	Normal	Cisco default. You can use this VLAN but you cannot delete it.	Yes
2–1001	Normal	For Ethernet VLANs; you can create, use, and delete these VLANs.	Yes
1002–1005	Normal	Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002–1005.	Yes
1006–4094	Extended	For Ethernet VLANs only.	No

The following information applies to VLAN ranges:

- Layer 3 LAN ports, WAN interfaces and subinterfaces, and some software features use internal VLANs in the extended range. You cannot use an extended range VLAN that has been allocated for internal use.
- With Release 12.1(13)E and later releases, to display the VLANs used internally, enter the **show vlan internal usage** command. With earlier releases, enter the **show vlan internal usage** and **show cwan vlans** commands.
- With Release 12.1(13)E and later releases, you can configure ascending internal VLAN allocation (from 1006 and up) or descending internal VLAN allocation (from 4094 and down). In previous 12.1EX releases that support 4096 VLANs, internal VLANs are allocated from 1006 and up.
- Switches running the Catalyst operating system do not support configuration of VLANs 1006–1024. If you configure VLANs 1006–1024, ensure that the VLANs do not extend to any switches running Catalyst software.
- You must enable the extended system ID to use extended range VLANs (see the "Understanding the Bridge ID" section on page 15-3).

Configurable VLAN Parameters

Note
- Ethernet VLAN 1 uses only default values.
- Except for the VLAN name, Ethernet VLANs 1006 through 4094 use only default values.
- With Release 12.1(13)E and later releases, you can configure the VLAN name for Ethernet VLANs 1006 through 4094.

You can configure the following parameters for VLANs 2 through 1001:

- VLAN name
- VLAN type (Ethernet, FDDI, FDDI network entity title [NET], TrBRF, or TrCRF)
- VLAN state (active or suspended)
- Security Association Identifier (SAID)
- Bridge identification number for TrBRF VLANs
- Ring number for FDDI and TrCRF VLANs
- Parent VLAN number for TrCRF VLANs
- Spanning Tree Protocol (STP) type for TrCRF VLANs

Understanding Token Ring VLANs

The following section describes the two Token Ring VLAN types supported on network devices running VTP version 2:

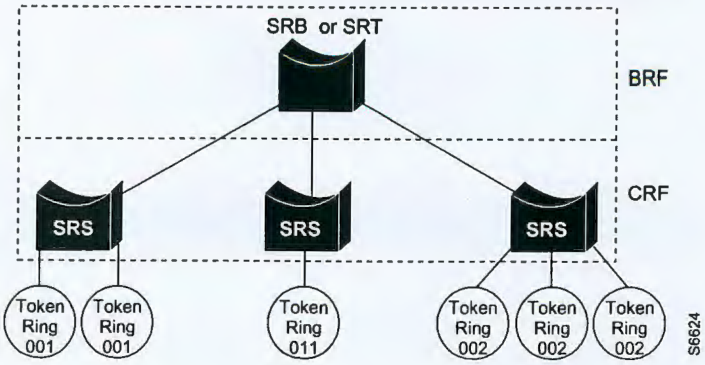
- Token Ring TrBRF VLANs, page 9-3
- Token Ring TrCRF VLANs, page 9-4

Note Catalyst 6500 series switches do not support Inter-Switch Link (ISL)-encapsulated Token Ring frames. When a Catalyst 6500 series switch is configured as a VTP server, you can configure Token Ring VLANs from the switch.

ken Ring TrBRF VLANs

Token Ring Bridge Relay Function (TrBRF) VLANs interconnect multiple Token Ring Concentrator Relay Function (TrCRF) VLANs in a switched Token Ring network (see Figure 9-1). The TrBRF can be extended across network devices interconnected with trunk links. The connection between the TrCRF and the TrBRF is referred to as a *logical port.*

Figure 9-1 Interconnected Token Ring TrBRF and TrCRF VLANs



For source routing, the Catalyst 6500 series switch appears as a single bridge between the logical rings. The TrBRF can function as a source-route bridge (SRB) or a source-route transparent (SRT) bridge running either the IBM or IEEE STP. If an SRB is used, you can define duplicate MAC addresses on different logical rings.

The Token Ring software runs an instance of STP for each TrBRF VLAN and each TrCRF VLAN. For TrCRF VLANs, STP removes loops in the logical ring. For TrBRF VLANs, STP interacts with external bridges to remove loops from the bridge topology, similar to STP operation on Ethernet VLANs.

⚠ **Caution** Certain parent TrBRF STP and TrCRF bridge mode configurations can place the logical ports (the connection between the TrBRF and the TrCRF) of the TrBRF in a blocked state. For more information, see the "VLAN Configuration Guidelines and Restrictions" section on page 9-8.

To accommodate IBM System Network Architecture (SNA) traffic, you can use a combination of SRT and SRB modes. In a mixed mode, the TrBRF determines that some ports (logical ports connected to TrCRFs) operate in SRB mode while other ports operate in SRT mode

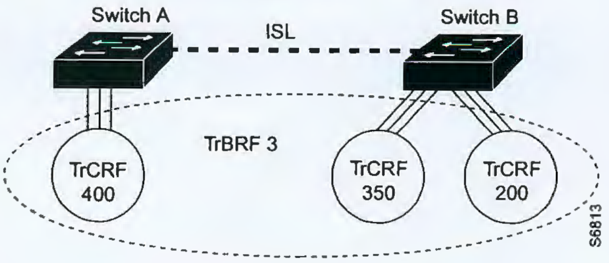
Token Ring TrCRF VLANs

Token Ring Concentrator Relay Function (TrCRF) VLANs define port groups with the same logical ring number. You can configure two types of TrCRFs in your network: undistributed and backup.

TrCRFs typically are undistributed, which means each TrCRF is limited to the ports on a single network device. Multiple undistributed TrCRFs on the same or separate network devices can be associated with a single parent TrBRF (see Figure 9-2). The parent TrBRF acts as a multiport bridge, forwarding traffic between the undistributed TrCRFs.

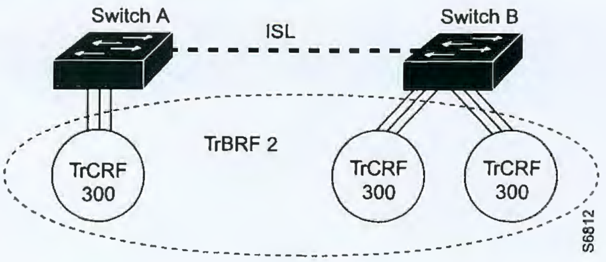
Note To pass data between rings located on separate network devices, you can associate the rings to the same TrBRF and configure the TrBRF for an SRB.

Figure 9-2 Undistributed TrCRFs



By default, Token Ring ports are associated with the default TrCRF (VLAN 1003, trcrf-default), which has the default TrBRF (VLAN 1005, trbrf-default) as its parent. In this configuration, a distributed TrCRF is possible (see Figure 9-3), and traffic is passed between the default TrCRFs located on separate network devices if the network devices are connected through an ISL trunk.

Figure 9-3 Distributed TrCRF



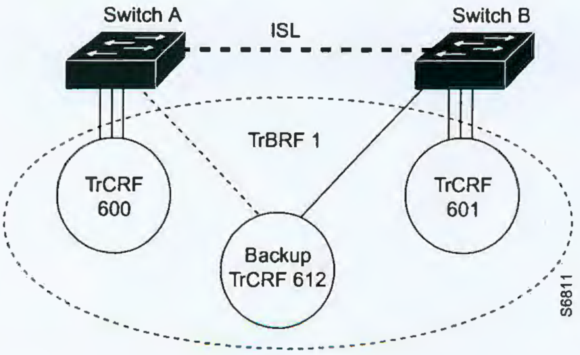
Within a TrCRF, source-route switching forwards frames based on either MAC addresses or route descriptors. The entire VLAN can operate as a single ring, with frames switched between ports within a single TrCRF.

You can specify the maximum hop count for All-Routes and Spanning Tree Explorer frames for each TrCRF. When you specify the maximum hop count, you limit the maximum number of hops an explorer is allowed to traverse. If a port determines that the explorer frame it is receiving has traversed more than the number of hops specified, it does not forward the frame. The TrCRF determines the number of hops an explorer has traversed by the number of bridge hops in the route information field.

If the ISL connection between network devices fails, you can use a backup TrCRF to configure an alternate route for traffic between undistributed TrCRFs. Only one backup TrCRF for a TrBRF is allowed, and only one port per network device can belong to a backup TrCRF.

If the ISL connection between the network devices fails, the port in the backup TrCRF on each affected network device automatically becomes active, rerouting traffic between the undistributed TrCRFs through the backup TrCRF. When the ISL connection is reestablished, all but one port in the backup TrCRF is disabled. Figure 9-4 illustrates the backup TrCRF.

Figure 9-4 Backup TrCRF



VLAN Default Configuration

Tables 9-2 through 9-6 show the default configurations for the different VLAN media types.

Table 9-2 Ethernet VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1	1–4094
VLAN name	"default" for VLAN 1 "VLAN*vlan_ID*" for other Ethernet VLANs	—
802.10 SAID	10*vlan_ID*	100001–104094
MTU size	1500	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Pruning eligibility	VLANs 2–1001 are pruning eligible; VLANs 1006–4094 are not pruning eligible.	—

Table 9-3 FDDI VLAN Defaults and Ranges

Parameter	Default	Range
VLAN ID	1002	1–1005
VLAN name	"fddi-default"	—
802.10 SAID	101002	1–4294967294
MTU size	1500	1500–18190
Ring number	0	1–4095
Parent VLAN	0	0–1005
Translational bridge 1	0	0–1005

Table 9-3 *FDDI VLAN Defaults and Ranges (continued)*

Parameter	Default	Range
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend

Table 9-4 *Token Ring (TrCRF) VLAN Defaults and Ranges*

Parameter	Default	Range
VLAN ID	1003	1–1005
VLAN name	"token-ring-default"	—
802.10 SAID	101003	1–4294967294
Ring Number	0	1–4095
MTU size	VTPv1 default 1500 VTPv2 default 4472	1500–18190
Translational bridge 1	0	0–1005
Translational bridge 2	0	0–1005
VLAN state	active	active, suspend
Bridge mode	srb	srb, srt
ARE max hops	7	0–13
STE max hops	7	0–13
Backup CRF	disabled	disable; enable

Table 9-5 *FDDI-Net VLAN Defaults and Ranges*

Parameter	Default	Range
VLAN ID	1004	1–1005
VLAN name	"fddinet-default"	—
802.10 SAID	101004	1–4294967294
MTU size	1500	1500–18190
Bridge number	1	0–15
STP type	ieee	auto, ibm, ieee
VLAN state	active	active, suspend

Table 9-6 *Token Ring (TrBRF) VLAN Defaults and Ranges*

Parameter	Default	Range
VLAN ID	1005	1–1005
VLAN name	"trnet-default"	—
802.10 SAID	101005	1–4294967294

Table 9-6 Token Ring (TrBRF) VLAN Defaults and Ranges (continued)

Parameter	Default	Range
MTU size	VTPv1 1500; VTPv2 4472	1500–18190
Bridge number	1	0–15
STP type	ibm	auto, ibm, ieee
VLAN state	active	active, suspend

VLAN Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when creating and modifying VLANs in your network:

- RPR+ redundancy (see Chapter 5, "Configuring RPR and RPR+ Supervisor Engine Redundancy") does not support a configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.
- You can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode. See the "VLAN Configuration Options" section on page 9-9.
- Before you can create a VLAN, the Catalyst 6500 series switch must be in VTP server mode or VTP transparent mode. For information on configuring VTP, see Chapter 8, "Configuring VTP."
- The VLAN configuration is stored in the vlan.dat file, which is stored in nonvolatile memory. You can cause inconsistency in the VLAN database if you manually delete the vlan.dat file. If you want to modify the VLAN configuration or VTP, use the commands described in this guide and in the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.
- To do a complete backup of your configuration, include the vlan.dat file in the backup.
- The Cisco IOS **end** command is not supported in VLAN database mode.
- You cannot enter **Ctrl-Z** to exit VLAN database mode.
- Catalyst 6500 series switches do not support Token Ring or FDDI media. The switch does not forward FDDI, FDDI-Net, TrCRF, or TrBRF traffic, but it can propagate the VLAN configuration through VTP.
- When a Catalyst 6500 series switch is configured as a VTP server, you can configure FDDI and Token Ring VLANs from the switch.
- You must configure a TrBRF before you configure the TrCRF (the parent TrBRF VLAN you specify must exist).
- In a Token Ring environment, the logical interfaces (the connection between the TrBRF and the TrCRF) of the TrBRF are placed in a blocked state if either of these conditions exists:
  - The TrBRF is running the IBM STP, and the TrCRF is in SRT mode.
  - The TrBRF is running the IEEE STP, and the TrCRF is in SRB mode.

Configuring VLANs

These sections describe how to configure VLANs:

- VLAN Configuration Options, page 9-9
- Creating or Modifying an Ethernet VLAN, page 9-10
- Assigning a Layer 2 LAN Interface to a VLAN, page 9-12
- Configuring the Internal VLAN Allocation Policy, page 9-12
- Mapping 802.1Q VLANs to ISL VLANs, page 9-12

Note

- With releases 12.1(11b)E and later, when you are in configuration mode you can enter EXEC mode commands by entering the **do** keyword before the EXEC mode command.
- VLANs support a number of parameters that are not discussed in detail in this section. For complete information, refer to the *Catalyst 6500 Series Switch Cisco IOS Command Reference* publication.

VLAN Configuration Options

These sections describe the VLAN configuration options:

- VLAN Configuration in Global Configuration Mode, page 9-9
- VLAN Configuration in VLAN Database Mode, page 9-9

VLAN Configuration in Global Configuration Mode

Note Releases 12.1(11b)E and later support VLAN configuration in global configuration mode.

If the switch is in VTP server or transparent mode (see the "Configuring VTP" section on page 8-6), you can configure VLANs in global and config-vlan configuration modes. When you configure VLANs in global and config-vlan configuration modes, the VLAN configuration is saved in the vlan.dat files. To display the VLAN configuration, enter the **show vlan** command.

If the switch is in VLAN transparent mode, use the copy **running-config startup-config** command to save the VLAN configuration to the startup-config file. After you save the running configuration as the startup configuration, use the **show running-config** and **show startup-config** commands to display the VLAN configuration.

Note

- When the switch boots, if the VTP domain name and VTP mode in the startup-config and vlan.dat files do not match, the switch uses the configuration in the vlan.dat file.
- You can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode.

VLAN Configuration in VLAN Database Mode

Note You cannot configure extended-range VLANs in VLAN database mode. You can configure extended-range VLANs only in global configuration mode. RPR+ redundancy does not support configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.

If the switch is in VTP server or transparent mode, you can configure VLANs in the VLAN database mode. When you configure VLANs in VLAN database mode, the VLAN configuration is saved in the vlan.dat files. To display the VLAN configuration, enter the **show vlan** command.

You use the interface configuration command mode to define the port membership mode and add and remove ports from a VLAN. The results of these commands are written to the running-config file, and you can display the file by entering the **show running-config** command.

Creating or Modifying an Ethernet VLAN

User-configured VLANs have unique IDs from 1 to 4094, except for reserved VLANs (see Table 9-1 on page 9-2). Enter the **vlan** command with an unused ID to create a VLAN. Enter the **vlan** command for an existing VLAN to modify the VLAN (you cannot modify an existing VLAN that is being used by a Layer 3 port or a software feature).

See the "VLAN Default Configuration" section on page 9-6 for the list of default parameters that are assigned when you create a VLAN. If you do not specify the VLAN type with the **media** keyword, the VLAN is an Ethernet VLAN.

To create or modify a VLAN, perform this task:

	Command	Purpose

Step 1	`Router# configure terminal`
	or
	`Router# vlan database`
		Enters VLAN configuration mode.

Step 2	`Router(config)# vlan vlan_ID{[-vlan_ID]|[,vlan_ID])`
	`Router(config-vlan)#`
	or
	`Router(vlan)# vlan vlan_ID`
		Creates or modifies an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs specified in a comma-separated list (do not enter space characters).

	`Router(config)# no vlan vlan_ID`
	`Router(config-vlan)#`
	or
	`Router(vlan)# no vlan vlan_ID`
		Deletes a VLAN.

Step 3	`Router(config-vlan)# end`
	or
	`Router(vlan)# exit`
		Updates the VLAN database and returns to privileged EXEC mode.

Step 4	`Router# show vlan [id | name] vlan`	Verifies the VLAN configuration.

When you create or modify an Ethernet VLAN, note the following syntax information:

- Releases 12.1(11b)E and later support VLAN configuration in global configuration mode.
- Releases 12.1(13)E and later support extended-range VLANs.
- RPR+ redundancy does not support a configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.

- Because Layer 3 ports and some software features require internal VLANs allocated from 1006 and up, configure extended-range VLANs starting with 4094.
- You can configure extended-range VLANs only in global configuration mode. You cannot configure extended-range VLANs in VLAN database mode.
- Layer 3 ports and some software features use extended-range VLANs. If the VLAN you are trying to create or modify is being used by a Layer 3 port or a software feature, the switch displays a message and does not modify the VLAN configuration.

When deleting VLANs, note the following syntax information:

- You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005.
- When you delete a VLAN, any LAN ports configured as access ports assigned to that VLAN become inactive. The ports remain associated with the VLAN (and inactive) until you assign them to a new VLAN.

This example shows how to create an Ethernet VLAN in global configuration mode and verify the configuration:

```
Router# configure terminal
Router(config)# vlan 3
Router(config-vlan)# end
Router# show vlan id 3

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
```

This example shows how to create an Ethernet VLAN in VLAN database mode:

```
Router# vlan database
Router(vlan)# vlan 3
VLAN 3 added:
    Name: VLAN0003
Router(vlan)# exit
APPLY completed.
Exiting....
```

This example shows how to verify the configuration:

```
Router# show vlan name VLAN0003
VLAN Name                             Status    Ports
---- -------------------------------- --------- ---------------------
3    VLAN0003                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- ------ ------
3    enet  100003     1500  -      -      -        -    0      0
Router#
```

Assigning a Layer 2 LAN Interface to a VLAN

A VLAN created in a management domain remains unused until you assign one or more LAN ports to the VLAN.

Note Make sure you assign LAN ports to a VLAN of the appropriate type. Assign Ethernet ports to Ethernet-type VLANs.

To assign one or more LAN ports to a VLAN, complete the procedures in the "Configuring LAN Interfaces for Layer 2 Switching" section on page 7-6.

Configuring the Internal VLAN Allocation Policy

Internal VLAN allocation policy is supported in Release 12.1(13)E and later releases. For more information about VLAN allocation, see the "VLAN Ranges" section on page 9-2.

Note The internal VLAN allocation policy is applied only following a reload.

To configure the internal VLAN allocation policy, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan internal allocation policy {ascending | descending}`	Configures the internal VLAN allocation policy.
	`Router(config)# no vlan internal allocation policy`	Returns to the default (ascending).
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# reload`	Applies the new internal VLAN allocation policy. ⚠ **Caution** You do not need to enter the **reload** command immediately. Enter the **reload** command during a planned maintenance window.

When you configure the internal VLAN allocation policy, note the following syntax information:

- Enter the **ascending** keyword to allocate internal VLANs from 1006 and up.
- Enter the **descending** keyword to allocate internal VLAN from 4094 and down.

This example shows how to configure descending as the internal VLAN allocation policy:

```
Router# configure terminal
Router(config)# vlan internal allocation policy descending
```

Mapping 802.1Q VLANs to ISL VLANs

The valid range of user-configurable ISL VLANs is 1 through 1001 and 1006 through 4094. The valid range of VLANs specified in the IEEE 802.1Q standard is 1 to 4094. You can map 802.1Q VLAN numbers to ISL VLAN numbers.

802.1Q VLANs in the range 1 through 1001 and 1006 through 4094 are automatically mapped to the corresponding ISL VLAN. 802.1Q VLAN numbers corresponding to reserved VLAN numbers must be mapped to an ISL VLAN in order to be recognized and forwarded by Cisco network devices.

These restrictions apply when mapping 802.1Q VLANs to ISL VLANs:

- You can configure up to eight 802.1Q-to-ISL VLAN mappings on the Catalyst 6500 series switch.
- You can only map 802.1Q VLANs to Ethernet-type ISL VLANs.
- Do not enter the native VLAN of any 802.1Q trunk in the mapping table.
- When you map an 802.1Q VLAN to an ISL VLAN, traffic on the 802.1Q VLAN corresponding to the mapped ISL VLAN is blocked. For example, if you map 802.1Q VLAN 1007 to ISL VLAN 200, traffic on 802.1Q VLAN 200 is blocked.
- VLAN mappings are local to each Catalyst 6500 series switch. Make sure you configure the same VLAN mappings on all appropriate network devices.

To map an 802.1Q VLAN to an ISL VLAN, perform this task:

	Command	Purpose
Step 1	`Router(config)# vlan mapping dot1q dot1q_vlan isl isl_vlan`	Maps an 802.1Q VLAN to an ISL Ethernet VLAN. The valid range for *dot1q_vlan* is 1001 to 4094. The valid range for *isl_vlan* is the same.
	`Router(config)# no vlan mapping dot1q {all | dot1q_vlan}`	Deletes the mapping.
Step 2	`Router(config)# end`	Exits configuration mode.
Step 3	`Router# show vlan`	Verifies the VLAN mapping.

This example shows how to map 802.1Q VLAN 1003 to ISL VLAN 200:

```
Router# configure terminal
Router(config)# vlan mapping dot1q 1003 isl 200
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show vlan
<...output truncated...>
802.1Q Trunk Remapped VLANs:
802.1Q VLAN    ISL VLAN
-----------   -----------
   1003          200
```

CHAPTER 1

Overview

The GigaStack GBIC (model WS-X3500-XL) adds port density and high-performance connectivity to supporting switches. When installed in a supporting switch, the GigaStack GBIC supports Gigabit connections in a cascaded stack or point-to-point configuration. The GigaStack GBIC autonegotiates the duplex setting of each port to maximize the bandwidth for your configuration.

Features

This section describes the GigaStack GBIC features:

- Half-duplex stacking using only one GBIC slot for each switch

  Stack up to nine switches to form an independent backbone that can be managed with a single IP address. This stack gives the appearance of a single large switch for network management purposes. For this kind of connectivity, see the "Example 1: Cascaded Stack Connection" section on page 1-9.

- Full-duplex connectivity between two switches

  You can also form a point-to-point link between two switches. The GigaStack GBIC supports one full-duplex link (in a point-to-point configuration) or up to eight half-duplex links (in a stack configuration) to other Gigabit Ethernet devices. For this kind of connectivity, see the "Example 2: Point-to-Point Connection" section on page 1-10.

- Support for redundant loop configurations in a GigaStack GBIC stack

  For more information, see the "Minimum IOS Release for Redundant Loop Configurations" section on page 1-7 and the "Cascaded Stack Connections with a Redundant Link" section on page 2-12
- Support for IOS Release 12.0(5)XU or later for Catalyst 2900 XL and 3500 XL switches, support for Release 12.1(6)EA2 or later for Catalyst 2950 switches, and support for Release 12.1(4)EA1 or later for Catalyst 3550 multilayer switches
- Management through the Cisco IOS command-line interface (CLI) or the web-based Cluster Management Suite (CMS)
- Field-replaceable

GigaStack GBIC LEDs

Figure 1-1 shows the LED locations on the GigaStack GBIC, and Table 1-1 describes the LED colors and their meanings.

Figure 1-1 GigaStack GBIC LEDs and Ports

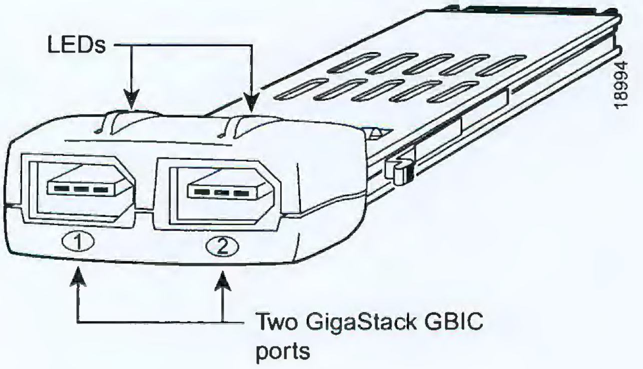


Table 1-1 GigaStack GBIC LEDs

Color	Meaning
Off	No link.
Green	Link present. This link occurs if there is connectivity with another network device and the GigaStack GBIC port.
Amber	Power-on self-test (POST) failure or use of an incorrect cable.
Flashing amber	Loop detection activated.

GBIC Module Slot LEDs

Figure 1-2 shows the GBIC module slot LED on the front of a supporting switch, and Figure 1-3 shows the GBIC LED location when the GigaStack GBIC is installed in the 1000BASE-X module.

Figure 1-2 GBIC Module Slot LED Location on a Switch

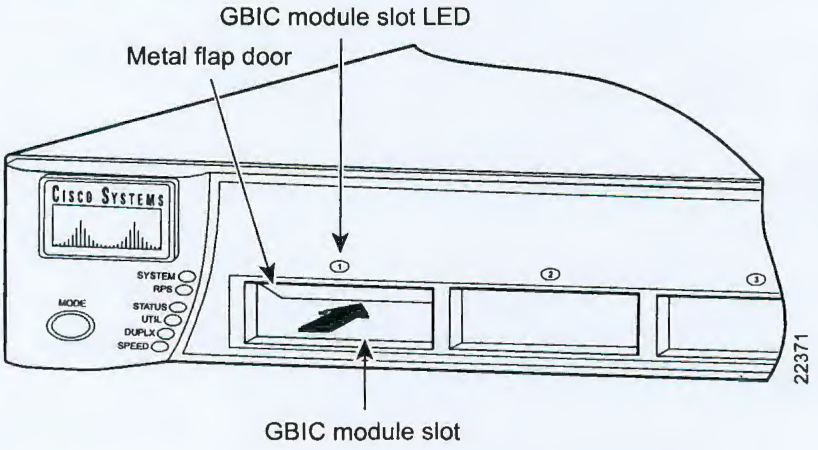


Figure 1-3 GBIC LED Location on a 1000BASE-X Module

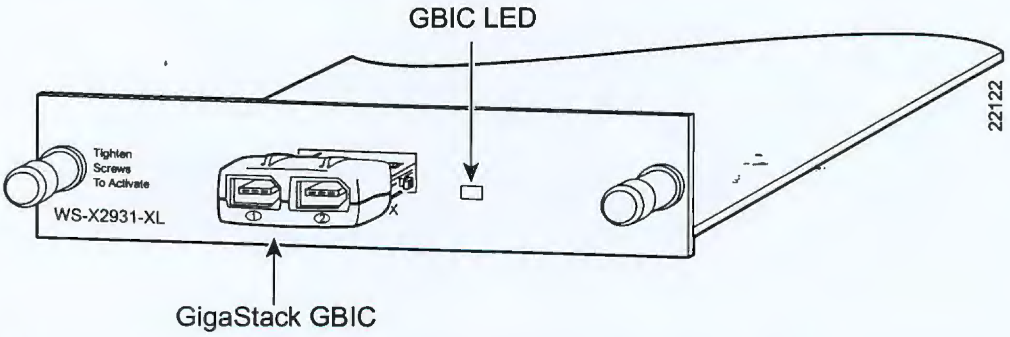


Table 1-2 describes the switch and 1000BASE-X module GBIC slot LED colors and port status.

Table 1-2 Switch and 1000BASE-X Module GBIC Slot LEDs

Color	Meaning
Off	No link, or port was administratively shut down.
Green	Link present.
Flashing green	Activity. Port is transmitting or receiving data.
Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, cyclic redundancy check (CRC) errors, and alignment and jabber errors are monitored for a link-fault indication.
Solid amber	Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data. **Note** After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
Flashing amber	Port is blocked by STP and is sending or receiving packets.

Cabling Guidelines

The GigaStack GBIC uses the following Cisco proprietary cables. See Figure 1-4 and Table 1-3 for more information.

The maximum distance for a GBIC-to-GBIC connection is 1 meter. The GigaStack GBIC requires Cisco proprietary signaling and cabling. For more information about cabling, see Appendix B, “Connectors and Cables.”

Figure 1-4 GigaStack GBIC Cables

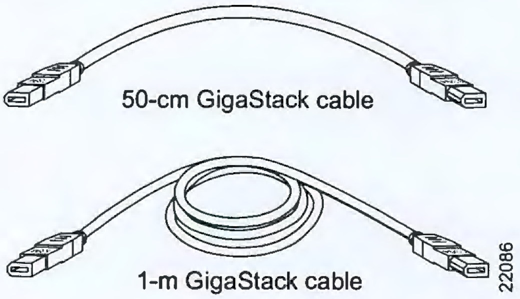


Table 1-3 GigaStack GBIC Cable Part Numbers

Part Number	Cable Length
CAB-GS-50CM	50 cm
CAB-GS-1M	1 m

The 50-cm cable comes with the GigaStack GBIC. You can order additional cables.

⚠ **Caution** Do not use standard IEEE 1394 cables with the GigaStack GBIC. You must use one of the Cisco proprietary cables (CAB-GS-50CM or CAB-GS-1M). If you use any other cable, you will not have connectivity.

⚠ **Caution** Do not use the GigaStack GBIC with standard IEEE 1394 equipment. You might damage the equipment or lose data.

Switches Supporting the GBIC

Refer to the online *GigaStack Gigabit Interface Converter Switch Compatibility Matrix* listed with the GBIC documentation on www.cisco.com for the most current list of products supporting the GBIC.

Caution Installing the GBIC in or connecting it to an unauthorized device might cause damage to the GBIC, the other device, or both.

Table 1-4 lists the switches and the module supporting the GigaStack GBIC.

Table 1-4 Switches and Module Supporting the GigaStack GBIC

Switch Series or Module	Model Number	Description
WS-X2931-XL module for Catalyst 2900 series XL switches	WS-X2931-XL	1 1000BASE-X port[1]
Catalyst 2900 XL switches	Catalyst 2912MF XL	12 100BASE-FX ports and 2 module slots
	Catalyst 2924M XL	24 autosensing 10/100 Ethernet ports and 2 module slots
Catalyst 2950 switches	Catalyst 2950G-12-EI	12 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 2950G-24-EI	24 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 2950G-24-EI-DC	24 autosensing 10/100 Ethernet ports and 2 GBIC module slots with DC-input power
	Catalyst 2950G-48-EI	48 autosensing 10/100 Ethernet ports and 2 GBIC module slots

Switch Series or Module	Model Number	Description
Catalyst 3500 XL switches	Catalyst 3508G XL	8 GBIC module slots
	Catalyst 3512 XL	12 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 3524 XL	24 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 3524 PWR XL	24 autosensing 10/100 inline-power Ethernet ports and 2 GBIC module slots
	Catalyst 3548 XL	48 autosensing 10/100 Ethernet ports and 2 GBIC module slots
Catalyst 3550 switches	Catalyst 3550-12G	2 autosensing 10/100/1000 Ethernet ports and 10 GBIC module slots
	Catalyst 3550-12T	10 autosensing 10/100/1000 Ethernet ports and 2 GBIC module slots
	Catalyst 3550-24-SMI Catalyst 3550-24-EMI	24 autosensing 10/100 Ethernet ports and 2 GBIC module slots
	Catalyst 3550-48-SMI Catalyst 3550-48-EMI	48 autosensing 10/100 Ethernet ports and 2 GBIC module slots

[1] The 1000BASE-X module provides one switched 1000-Mbps port in half-duplex, full-duplex, or autonegotiation mode for a GigaStack GBIC. The port supports the IEEE 802.3Z 1000BASE-X standard.

Minimum IOS Release for Redundant Loop Configurations

To ensure support for redundant loop configurations when using the GigaStack GBIC in a cascaded stack configuration, make sure that every switch in the stack is running at least the minimum IOS Release listed in Table 1-5.

Table 1-5 Minimum IOS Release for Redundant Loop Configurations

Supported Switch	Minimum IOS Release
Modular 2900 XL switches	12.0(5)XU (April 2000)
2950 switches	12.1(6)EA2 (December 2000)
3500 XL switches	12.0(5)XU (April 2000)
3550 multilayer switches	12.1(4)EA1 (May 2001)

Note All switches in a series must run the same software version. For example, if the stack includes only Catalyst 2900 series XL and 3500 series XL switches, they must run Release 12.0(5)XU or later. If the stack includes a mixture of Catalyst 2900 series XL, 3500 series XL, 2950, and 3550 switches, all the 2900 XL and 3500 XL switches must run Release 12.0(5)XW or later, all the Catalyst 2950 switches must run Release 12.1(6)EA2 or later, and all the Catalyst 3550 switches must run Release 12.1(4)EA1 or later.

For more information, see the "Cascaded Stack Connections with a Redundant Link" section on page 2-12. For switch software upgrade information, refer to the release notes for your switch.

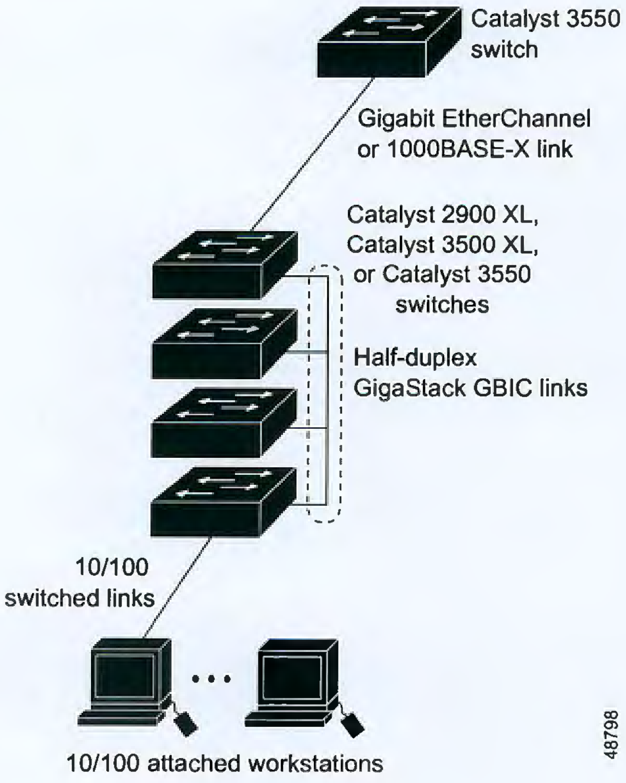
Deployment Examples

This section contains examples that use the GigaStack GBIC as a Gigabit uplink to aggregate traffic in a switched and shared network.

Example 1: Cascaded Stack Connection

Figure 1-5 shows the GigaStack GBIC cascaded in a half-duplex stack configuration.

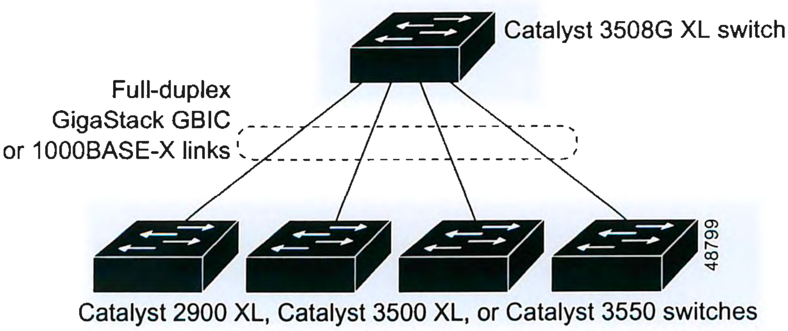
Figure 1-5 Cascaded Stack Connection


Catalyst 3550 switch
Gigabit EtherChannel or 1000BASE-X link
Catalyst 2900 XL, Catalyst 3500 XL, or Catalyst 3550 switches
Half-duplex GigaStack GBIC links
10/100 switched links
10/100 attached workstations
48798

Example 2: Point-to-Point Connection

Figure 1-6 shows the 3500 XL switch aggregating traffic by using a GigaStack GBIC as a full-duplex, point-to-point uplink connection.

Figure 1-6 Point-to-Point Connection



Apêndice FL

CHAPTER 3

Installation

This chapter describes how to install your switch, interpret the power-on self-test (POST), and connect the switch to other devices. Read these topics, and perform the procedures in this order:

Preparing for Installation

This section provides information about these topics:

- Warnings, page 3-2
- EMC Regulatory Statements, page 3-4
- Installation Guidelines, page 3-7
- Verifying Package Contents, page 3-8

Warnings

These warnings are translated into several languages in Appendix D, “Translat Safety Warnings.”

Warning **This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.**

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.**

Warning **Only trained and qualified personnel should be allowed to install or replace this equipment.**

Warning **Read the installation instructions before you connect the system to its power source.**

Warning **Unplug the power cord before you work on a system that does not have an on/off switch.**

Warning

Do not stack the chassis on any other equipment. If the chassis falls, it can cause severe bodily injury and equipment damage.

Warning

To comply with safety regulations, mount switches on a wall with the front panel facing up.

Warning

If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.

Warning

The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.

Warning

To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 113°F (45°C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.

Warning

When installing the unit, always make the ground connection first and disconnect it last.

Warning

This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.

Warning

Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.**

Warning **Attach only the Cisco RPS (model PWR300-AC-RPS-N1) to the RPS receptacle.**

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.**

Warning **Class 1 laser product**

Warning **Avoid direct exposure to the laser beam**

EMC Regulatory Statements

This section includes specific regulatory statements about the Catalyst 2950 switches.

U.S.A.

U.S. regulatory information for this product is in the front matter of this manual.

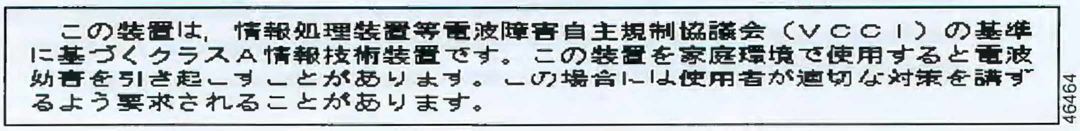
Taiwan

Warning **This is a Class A Information Product, when used in residential environment, it may cause radio frequency interference, under such circumstances, the user may be requested to take appropriate countermeasures.**

警告 這是甲類資訊產品，在居住環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Japan

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.


この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

46464

Korea

Warning — This is a Class A Device and is registered for EMC requirements for industrial use. The seller or buyer should be aware of this. If this type was sold or purchased by mistake, it should be replaced with a residential-use type.

주의 — A급 기기 이 기기는 업무용으로 전자파 적합 등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Hungary

Warning — This equipment is a class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022). Class A equipment is designed for typical commercial establishments for which special conditions of installation and protection distance are used.

Figyelmeztetés — Figyelmeztetés a felhasználói kézikönyv számára: Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfeleleoen kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelo kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelo speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.

Installation Guidelines

When determining where to place the switch, observe these guidelines.

- Before installing the switch, first verify that the switch is operational by powering it on and running POST. Follow the procedures in the "Verifying Switch Operation" section on page 3-10.
- For 10/100 ports and 10/100/1000 ports, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).
- For 100BASE-FX ports, the cable length from a switch to an attached device cannot exceed 6562 feet (2 kilometers).
- For 1000BASE-SX ports and 1000BASE-SX Gigabit Interface Converter (GBIC) module ports, the cable length from a switch to an attached device cannot exceed 1804 feet (550 meters).
- For 1000BASE-LX/LH GBIC module ports, the cable length from a switch to an attached device cannot exceed 32,810 feet (10 kilometers).
- For 1000BASE-ZX GBIC module ports, the cable length from a switch to an attached device cannot exceed 328,100 feet (100 kilometers).
- For 1000BASE-T GBIC module ports, the cable length from a switch to an attached device cannot exceed 328 feet (100 meters).
- For Coarse Wave Division Multiplexing (CWDM) GBIC module ports, the cable length from a switch to an attached device cannot exceed 393,719 feet (120 kilometers). For specific cable lengths, refer to the CWDM GBIC module documentation.
- For GigaStack GBIC module ports, the cable length from a switch to an attached device cannot exceed 3 feet (1 meter).
- For Long-Reach Ethernet (LRE) ports, cable-length specifications vary. See the "LRE Port" section on page 2-12.
- Operating environment is within the ranges listed in Appendix A, "Technical Specifications."
- Clearance to front and rear panels meet these conditions:
  - Front-panel LEDs can be easily read.
  - Access to ports is sufficient for unrestricted cabling.
  - Rear-panel AC power connector on switches other than the LRE switches is within reach of an AC power outlet.

  - Rear-panel direct current (DC) power connector on the Catalyst 2950G-24-EI-DC switch is within reach of a circuit breaker.
  - Front-panel AC power connector on the LRE switches is within reach of an AC power outlet.
  - Front-panel DC power connector on the Catalyst 2950ST-24 LRE 997 switch is within reach of a circuit breaker.
- Airflow around the switch and through the vents is unrestricted.
- Temperature around the unit does not exceed 113°F (45°C).

Note If the switch is installed in a closed or multirack assembly, the temperature around it might be greater than normal room temperature.

- Cabling is away from sources of electrical noise, such as radios, power lines, and fluorescent lighting fixtures.

Verifying Package Contents

Note Carefully remove the contents from the shipping container, and check each item for damage. If any item is missing or damaged, contact your Cisco representative or reseller for support. Return all packing materials to the shipping container and save them.

The switch is shipped with these items:

- This *Catalyst 2950 Desktop Switch Hardware Configuration Guide*
- *About the Catalyst 2950 and Catalyst 2955 Documentation*
- AC power cord (not shipped with the Catalyst 2950G-24-EI-DC switch or the Catalyst 2950ST-24 LRE 997 switch)
- Mounting kit containing these items:
  - Four rubber feet for mounting the switch on a table, shelf, or desk
  - Two 19-inch or 24-inch rack-mounting brackets

  - Six number-8 Phillips flat-head screws for attaching the brackets to the switch
  - Four number-8 Phillips truss-head screws for attaching the brackets to the switch
  - Four number-12 Phillips machine screws for attaching the brackets to a rack
  - One cable guide and one black Phillips machine screw for attaching the cable guide to one of the mounting brackets
  - One RPS connector cover and two number-4 pan-head screws
- DC-switch kit containing these items:
  - One DC terminal block plug (also called a terminal block header)
  - One ground lug
  - Two number-10-32 screws for attaching the ground lug to the switch
  - Two 23-inch rack-mounting brackets (with 1-inch spacing for telco racks)
  - Four number-8 Phillips truss-head screws for attaching the brackets to the switch
  - Two number-12 Phillips machine screws for attaching the brackets to a rack

Note The DC-switch kit ships only with the Catalyst 2950G-24-EI-DC or Catalyst 2950ST-24 LRE 997 switch.

- One RJ-45-to-DB-9 adapter cable
- Product ownership registration card

If you want to connect a terminal to the switch console port, you need to provide an RJ-45-to-DB-25 female DTE adapter. You can order a kit (part number ACS-DSBUASYN=) with that adapter from Cisco.

Verifying Switch Operation

Before installing the switch in a rack, on a wall, or on a table or shelf, you should power on the switch and verify that the switch passes POST. See Chapter 1, "Quick Installation," for the steps required to connect a PC to the switch console port and to power on the switch.

After a successful POST, follow these steps:

Step 1 Turn off power to the switch.

Step 2 Disconnect the cables.

Step 3 Determine where you want to install the switch.

Installing the Switch in a Rack

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Note Figure 3-1 to Figure 3-20 show the Catalyst 2950-24, 2950G-24-EI-DC, and 2950G-48-EI switches as examples. You can install other Catalyst 2950 switches in a rack as shown in these illustrations.

To install the switch in a 19-, 23-, or 24-inch rack, follow these steps:

1. Attaching the Brackets to the Switch, page 3-11
2. Mounting the Switch in a Rack, page 3-21
3. Attaching the Optional Cable Guide, page 3-22

Note Installing the Catalyst 2950G-48-EI switch in a 23-inch or 24-inch rack requires an optional bracket kit not included with the switch. You can order a kit containing the 23-inch or 24-inch rack-mounting brackets and hardware from Cisco (part number RCKMNT-1RU=).

Attaching the Brackets to the Switch

The bracket orientation and the screws that you use depend on whether you are attaching the brackets to a 19-, 23-, or 24-inch rack. Follow these guidelines:

- When mounting a switch other than a Catalyst 2950G-48-EI switch in a 19-inch rack, use two Phillips flat-head screws to attach the long side of the 19- or 24-inch bracket to the switch. See Figure 3-1, Figure 3-2, and Figure 3-3.
- When mounting a Catalyst 2950G-48-EI switch in a 19-inch rack, use three Phillips flat-head screws to attach the long side of the 19- or 24-inch bracket to the switch. See Figure 3-4, Figure 3-5, and Figure 3-6.
- When mounting a Catalyst 2950G-24-EI-DC or Catalyst 2950ST-24 LRE 997 switch in a 23-inch rack, use two Phillips truss-head screws to attach the 23-inch bracket to the switch. See Figure 3-7, Figure 3-8, and Figure 3-9.
- When mounting a switch other than a Catalyst 2950G-48-EI switch in a 24-inch rack, use two Phillips truss-head screws to attach the 19- or 24-inch bracket to the switch. See Figure 3-10, Figure 3-11, and Figure 3-12.
- When mounting a Catalyst 2950G-48-EI switch in a 24-inch rack, use three Phillips flat-head screws to attach the 24-inch bracket (part number RCKMNT-1RU=) to the switch. See Figure 3-13, Figure 3-14, and Figure 3-15.

Figure 3-1 to Figure 3-15 show how to attach a bracket to one side of the switch. Follow the same steps to attach the second bracket to the opposite side of the switch.

Figure 3-1 Attaching Brackets on the Switch in a 19-Inch Rack (Front Panel Forward)

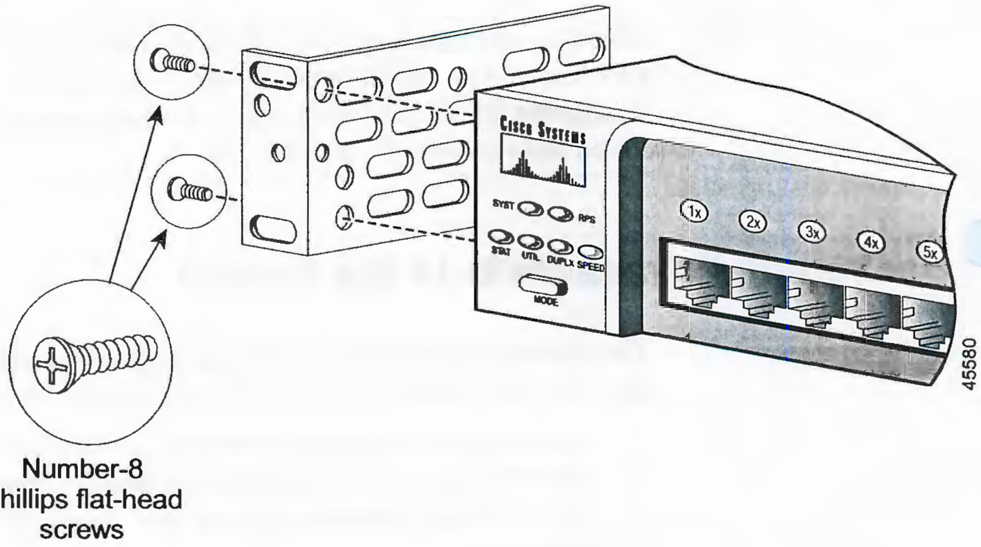


Figure 3-2 *Attaching Brackets on the Switch in a 19-Inch Rack (Rear Panel Forward)*

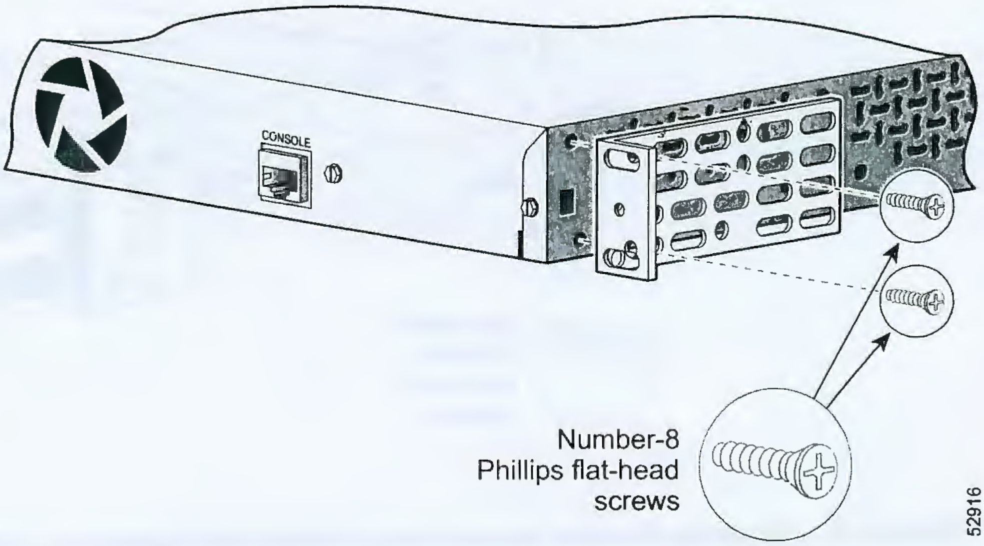


Figure 3-3 *Attaching Brackets on the Switch in a 19-Inch Telco Rack*

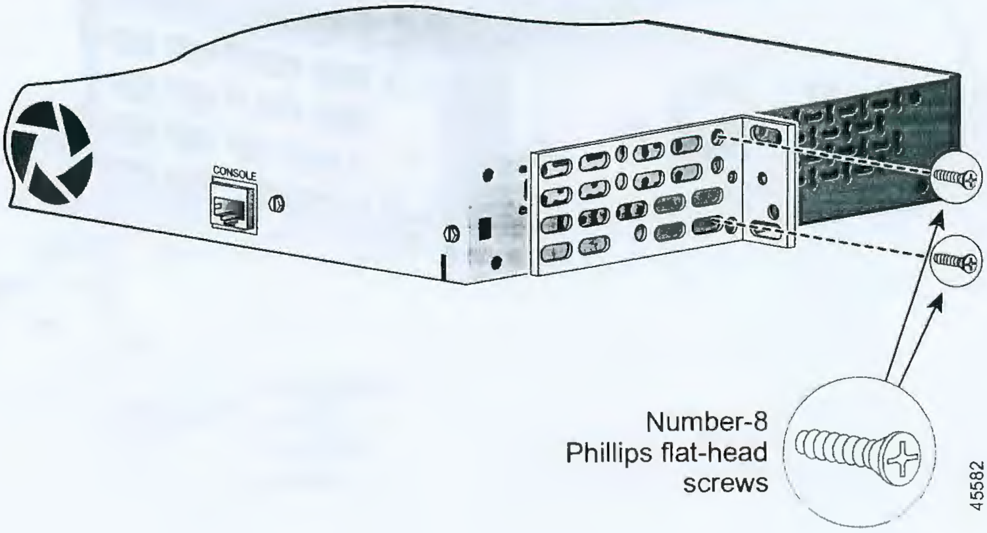


Figure 3-4 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Front Panel Forward)

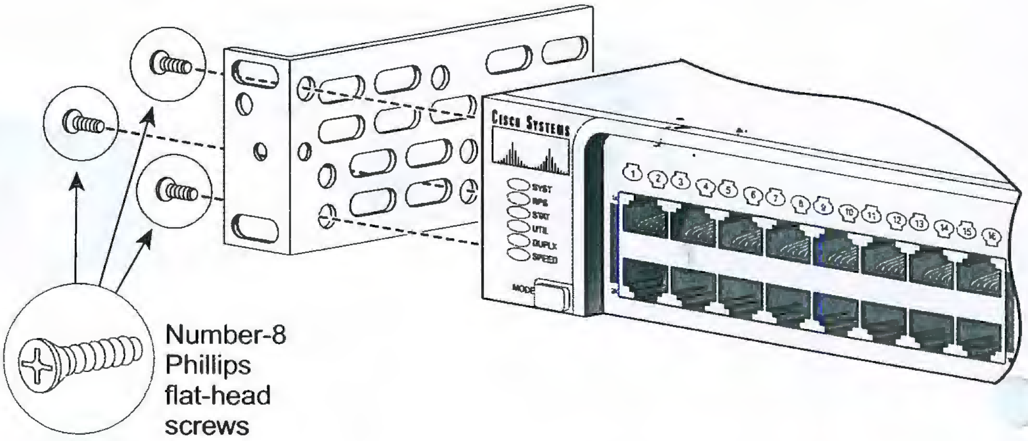


Figure 3-5 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Rack (Rear Panel Forward)

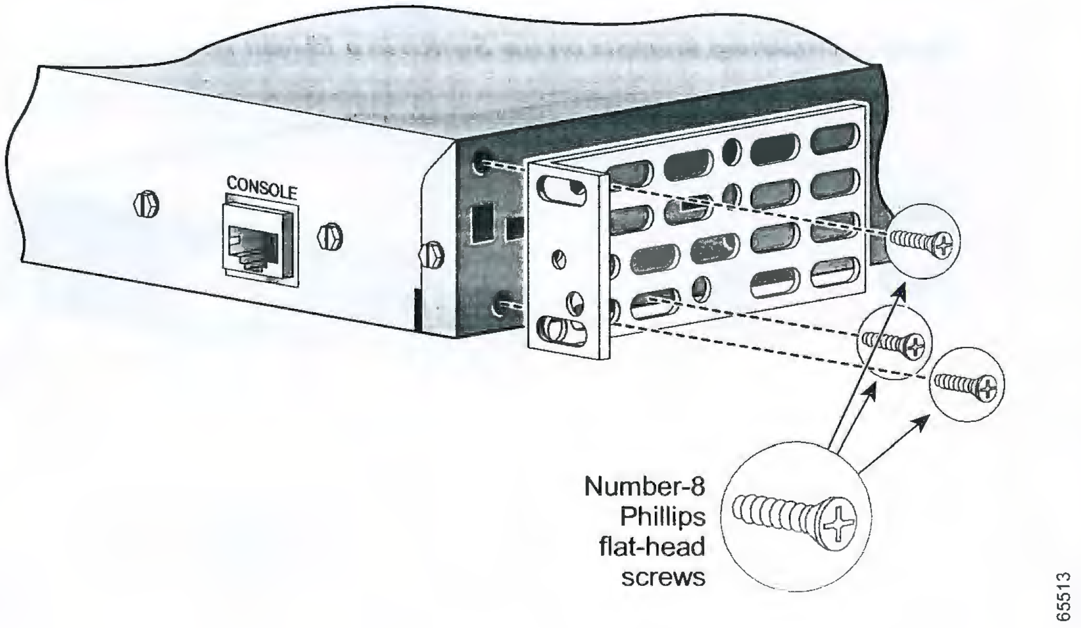


Figure 3-6 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 19-Inch Telco Rack

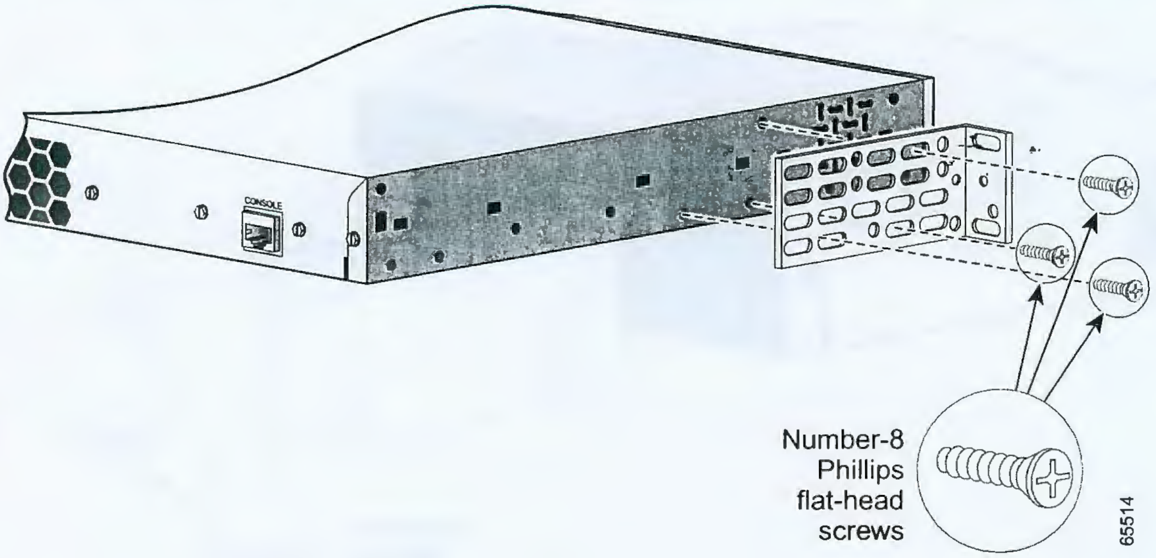


Figure 3-7 Attaching Brackets on the Catalyst 2950G-24-EI-DC or 2950ST-24 LRE 997 Switch in a 23-Inch Telco Rack (Front Panel Forward)

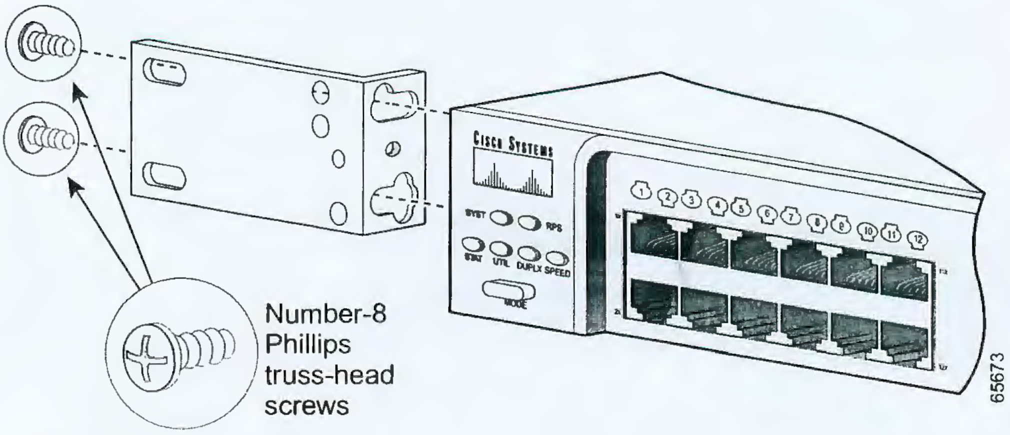


Figure 3-8 Attaching Brackets on the Catalyst 2950G-24-EI-DC or 2950ST-24 LRE 997 Switch in a 23-Inch Telco Rack (Rear Panel Forward)

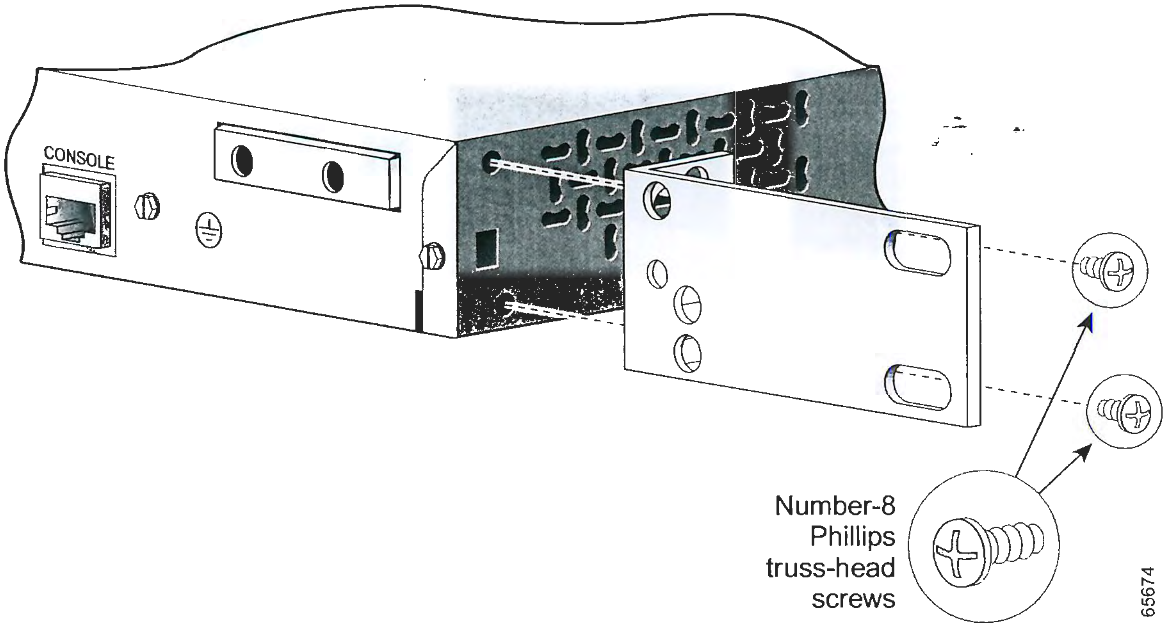


Figure 3-9 Attaching Brackets on the Catalyst 2950G-24-EI-DC or 2950ST-24 LRE 997 Switch in a 23-Inch Telco Rack

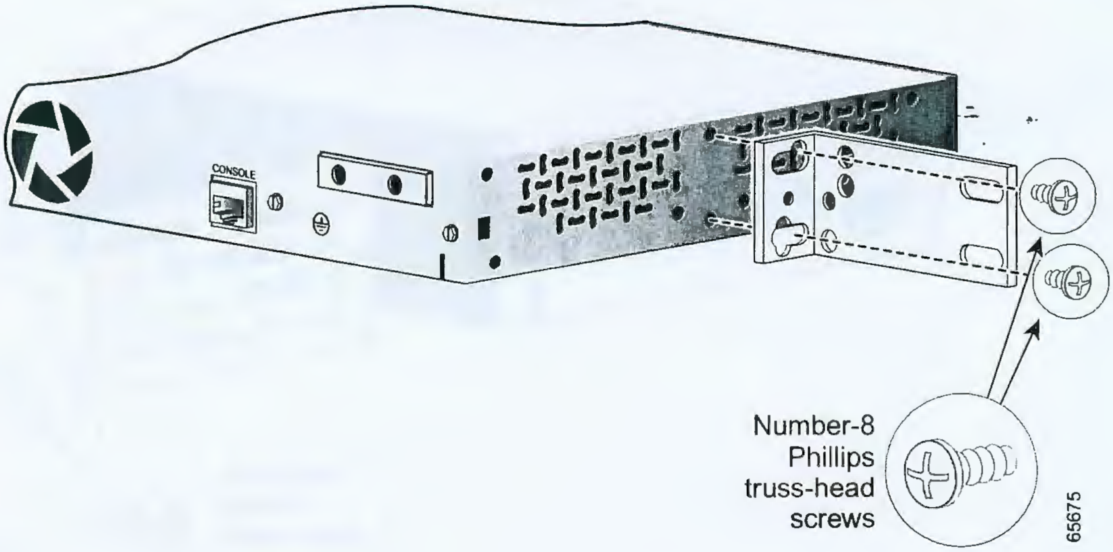


Figure 3-10 Attaching Brackets on the Switch in a 24-Inch Rack (Front Panel Forward)

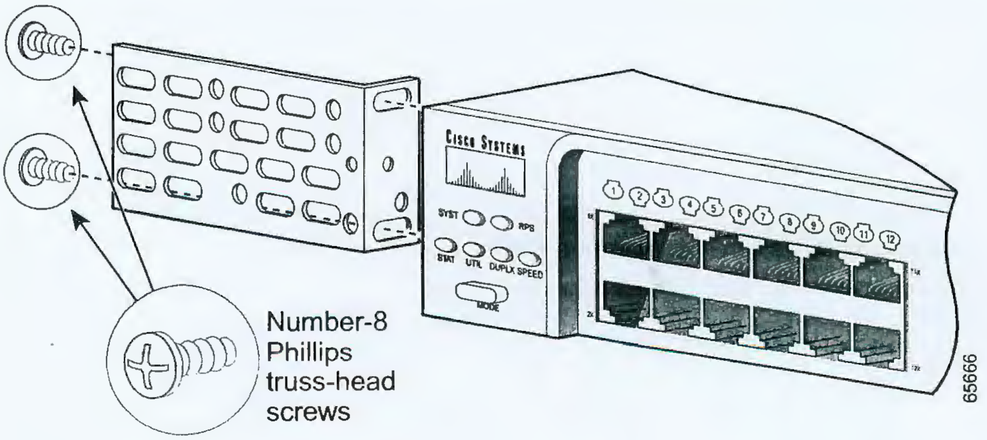


Figure 3-11 Attaching Brackets on the Switch in a 24-Inch Rack (Rear Panel Forward)

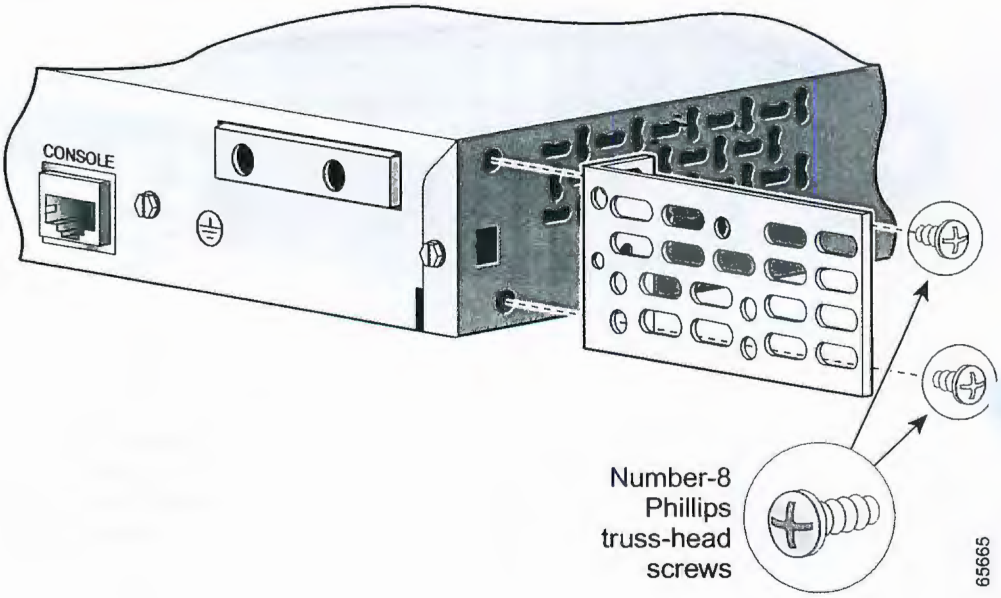


Figure 3-12 Attaching Brackets on the Switch in a 24-Inch Telco Rack

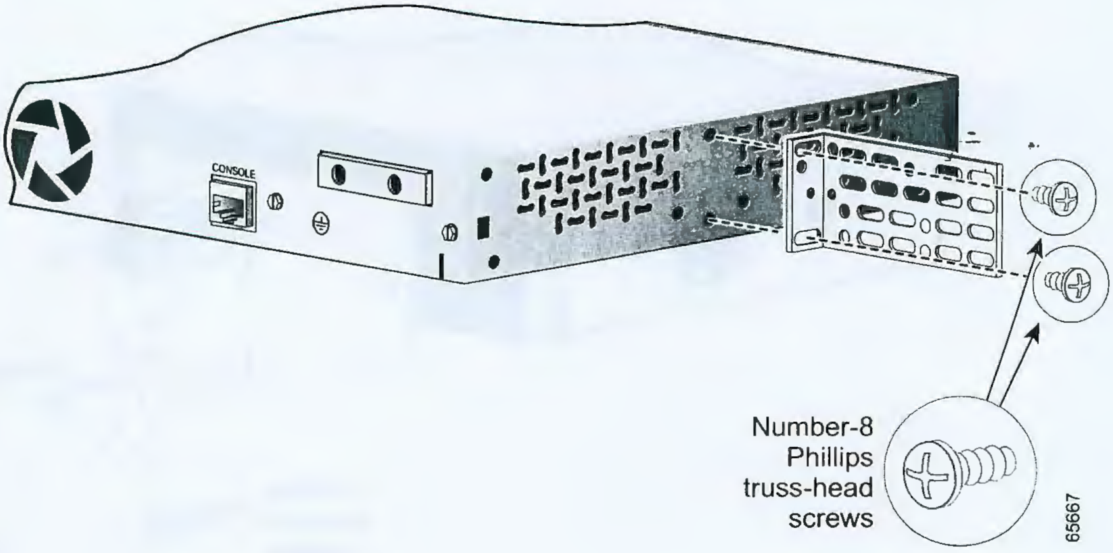


Figure 3-13 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Front Panel Forward)

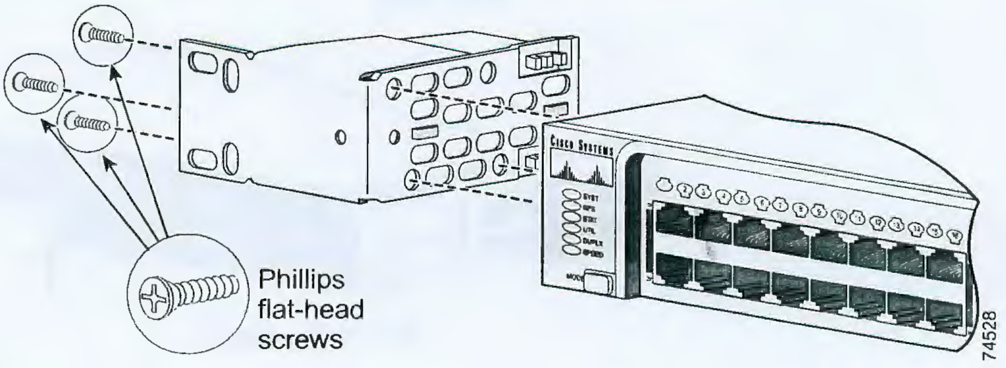


Figure 3-14 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Rack (Rear Panel Forward)

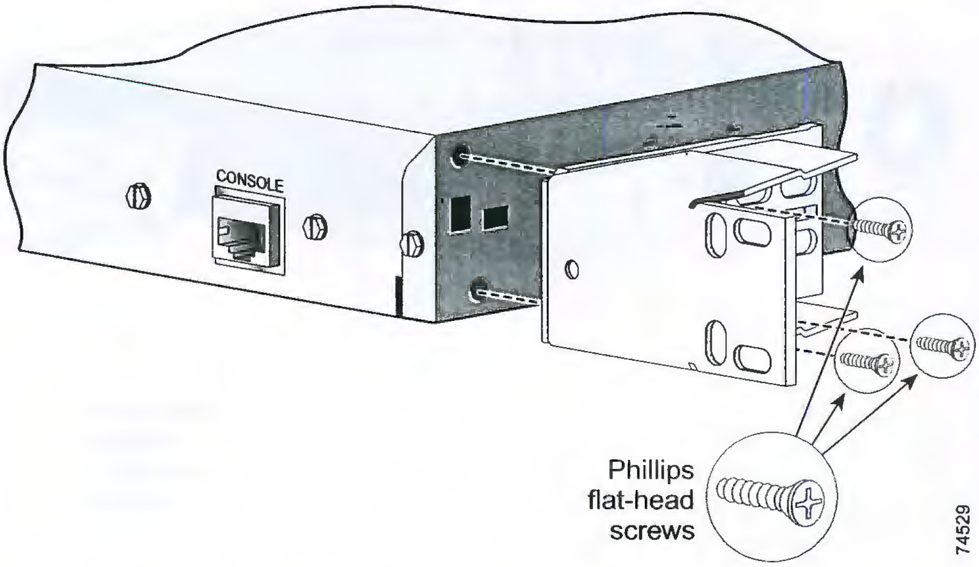
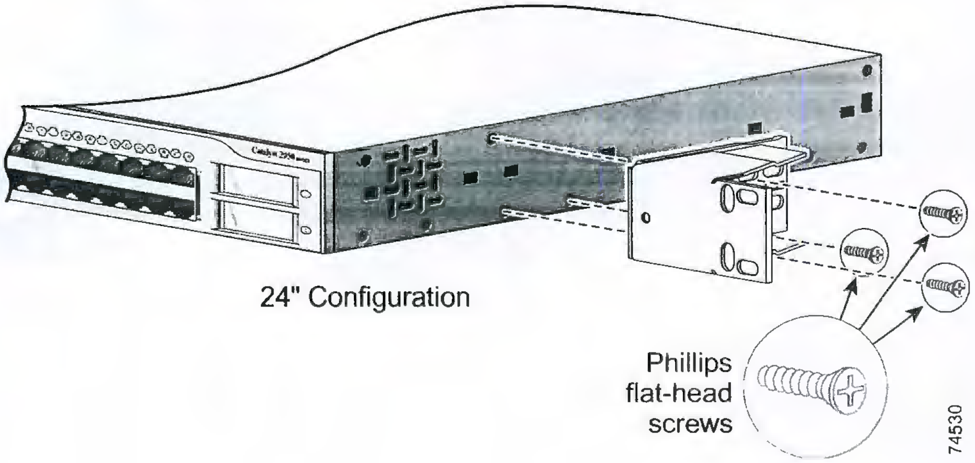


Figure 3-15 Attaching Brackets on the Catalyst 2950G-48-EI Switch in a 24-Inch Telco Rack

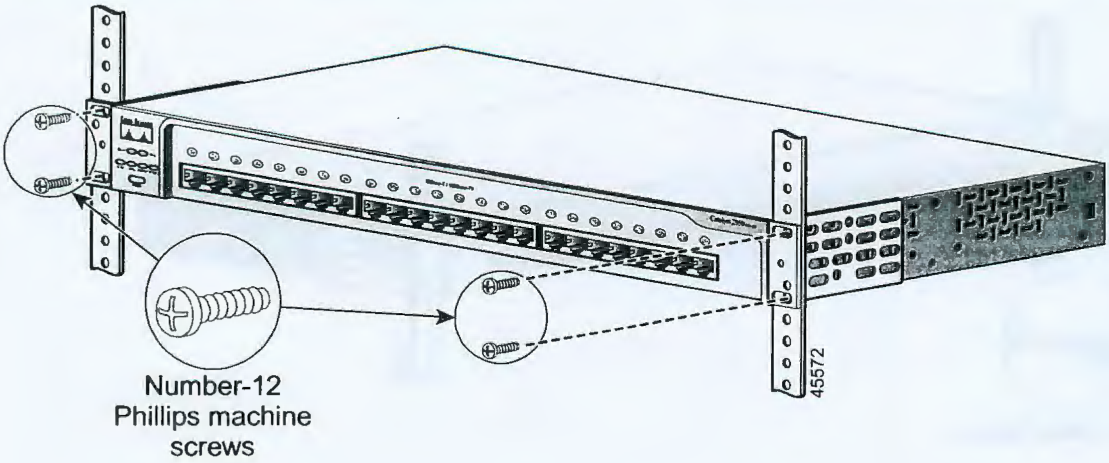


Mounting the Switch in a Rack

After attaching the brackets, use the four Phillips machine screws to securely attach the brackets to the rack, as shown in Figure 3-16.

When installing a switch other than an LRE switch, to prevent the cables from obscuring the switch and other devices in the rack, you can also attach the cable guide to the rack. See the"Attaching the Optional Cable Guide" section for instructions.

Figure 3-16 Mounting the Switch in a Rack



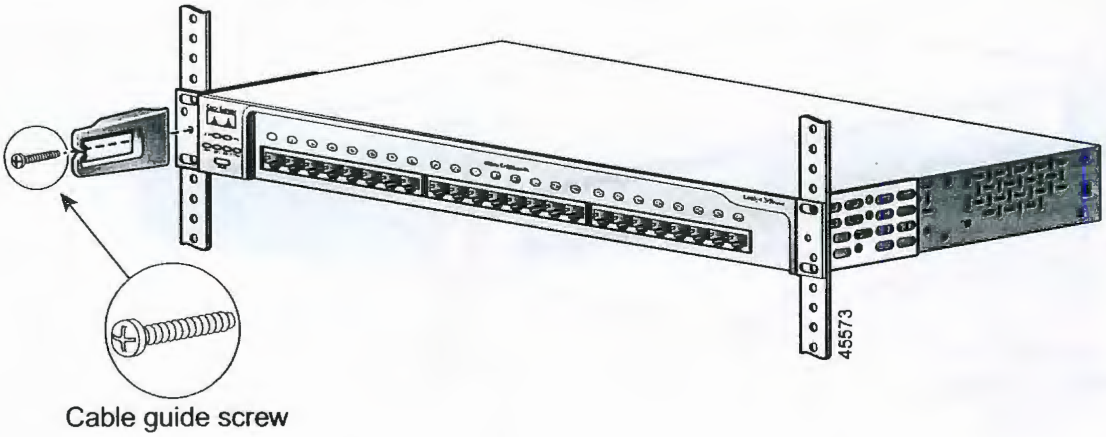
After mounting the switch in the rack, start the terminal-emulation software, and provide power to the switch. See Chapter 1, "Quick Installation" for instructions.

Attaching the Optional Cable Guide

We recommend attaching the cable guide to prevent the cables from obscuring the front panels of the switch and other devices installed in the rack. Use the supplied black Phillips machine screw to attach the cable guide to the left or right bracket, as shown in Figure 3-17.

Note You cannot use the cable guide with Catalyst 2950 LRE switches.

Figure 3-17 Attaching the Cable Guide



Installing the Switch on a Table, Shelf, or Desk

Before placing the switch on a table, shelf, or desk, locate the adhesive strip w rubber feet in the mounting-kit envelope, and attach four rubber feet to the recessed areas on the switch bottom. Place the switch on a table, shelf, or desk near an AC power source or DC-input power source.

Start the terminal-emulation software and provide power to the switch. See Chapter 1, "Quick Installation," for instructions.

Installing the Switch on a Wall

Warning **To comply with safety regulations, mount switches on a wall with the front panel facing up.**

Warning **If a redundant power system (RPS) is not connected to the switch, install an RPS connector cover on the back of the switch.**

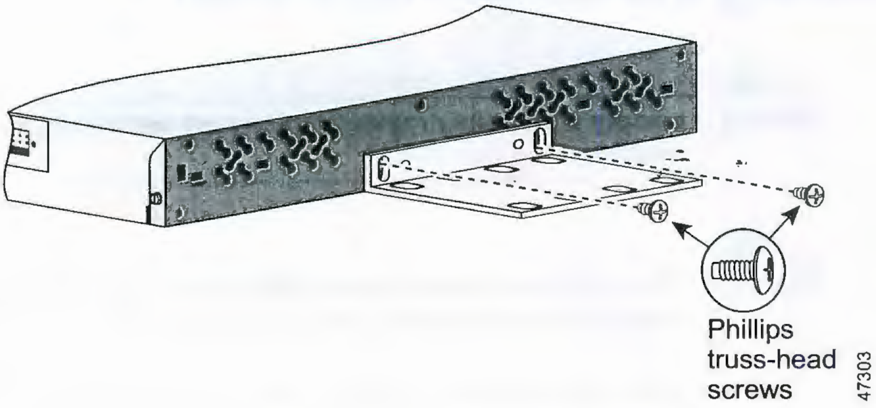
You can mount the Catalyst 2950 switch to a wall in a face-up configuration. To attach the switch to a wall, follow the procedures in this section.

1. Attaching the Brackets to the Switch, page 3-23
2. Attaching the RPS Connector Cover, page 3-24
3. Mounting the Switch to a Wall, page 3-25

Attaching the Brackets to the Switch

Use the supplied Phillips flat-head screws to attach a bracket to the switch. Figure 3-18 shows how to attach the bracket to one side of the switch. Follow the same steps to attach the second bracket to the opposite side of the switch.

Figure 3-18 Attaching Brackets for Wall-Mounting for the Catalyst 2950 Switch

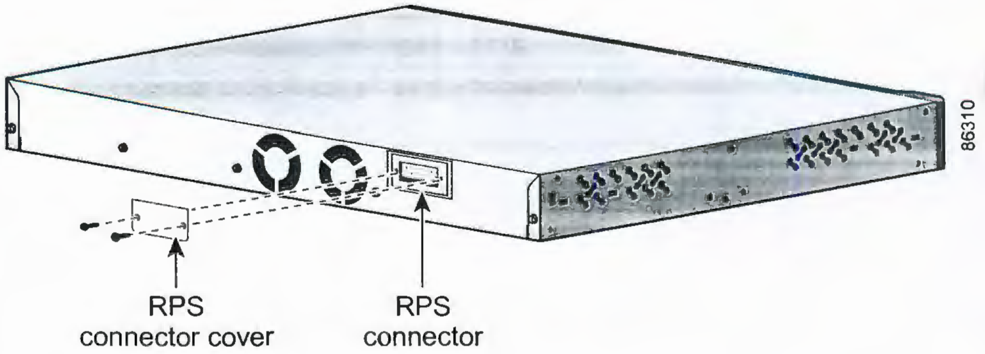


Attaching the RPS Connector Cover

If you are not using a redundant power system (RPS) with your switch, use two number-4 Phillips pan-head screws to install an RPS connector cover to the back of the switch. (See Figure 3-19.) The pan-head screws are included in the accessory kit.

Warning **If an RPS is not connected to the switch, install an RPS connector cover on the back of the switch.**

Figure 3-19 Attaching the RPS Connector Cover

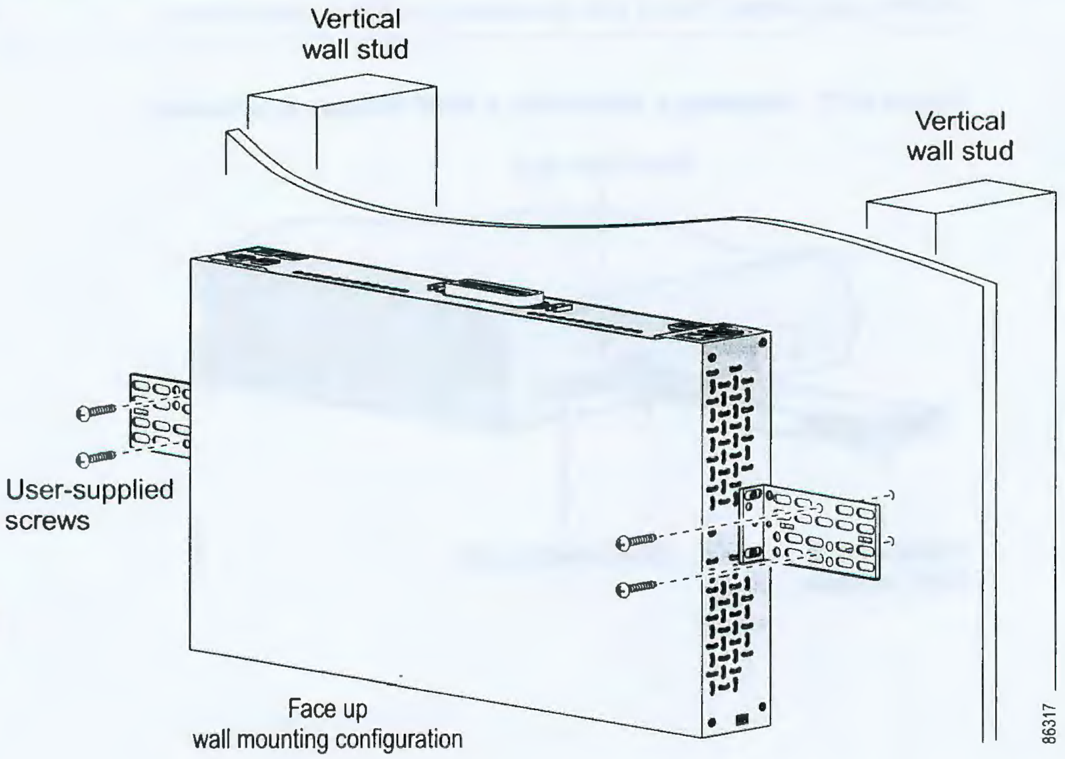


Mounting the Switch to a Wall

Warning **To comply with safety regulations, mount switches on a wall with the front panel facing up.**

For the best support of the switch and cables, make sure the switch is attached securely to a wall stud or to a firmly attached plywood mounting backboard, as shown in Figure 3-20.

Figure 3-20 Mounting a Catalyst 2950 Switch to a Wall



After the switch is mounted on the wall, power the switch as described in Chapter 1, "Quick Installation."

Installing the GBIC Modules

Figure 3-21, Figure 3-22, and Figure 3-23 show how to insert a GBIC module in a GBIC module slot on the switch. For instructions on how to install a CWDM GBIC module in a GBIC module slot, refer to the documentation that came with that GBIC module.

For detailed instructions on installing, removing, and cabling the GBIC module (the 1000BASE-X module, the 1000BASE-T module, the CWDM GBIC module, or the GigaStack module), refer to your GBIC documentation.

⚠ **Caution** To prevent electrostatic-discharge (ESD) damage when installing GBIC modules, follow your normal board and component handling procedures.

Figure 3-21 Installing a 1000BASE-X GBIC Module in a Switch

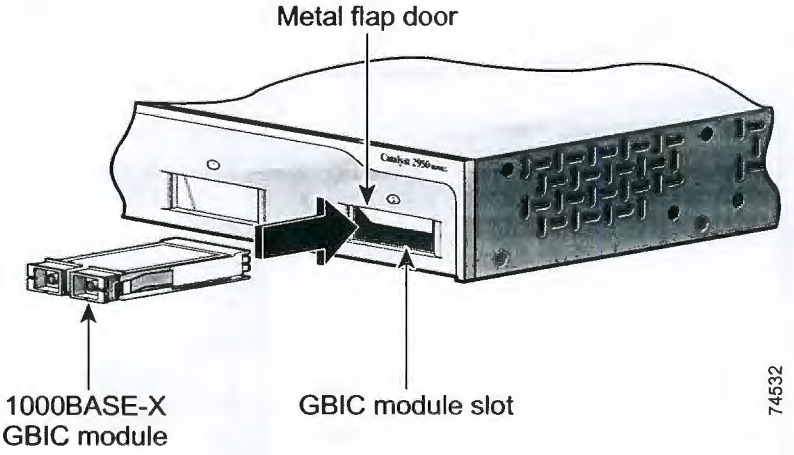


Figure 3-22 Installing a 1000BASE-T GBIC Module in a Switch

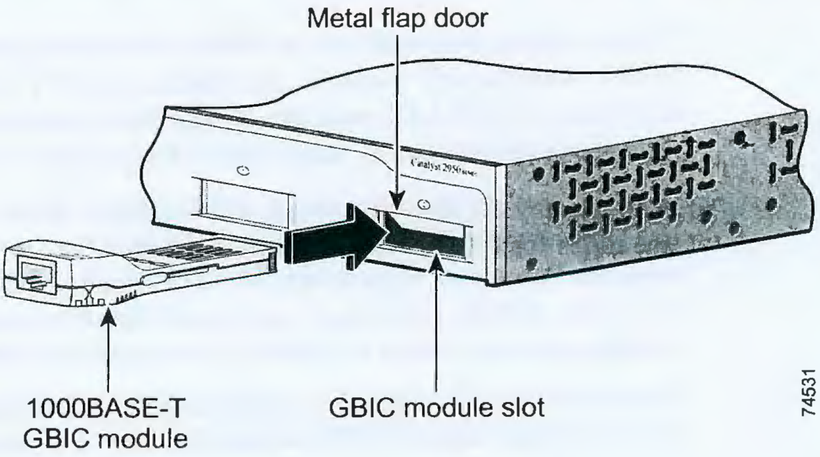
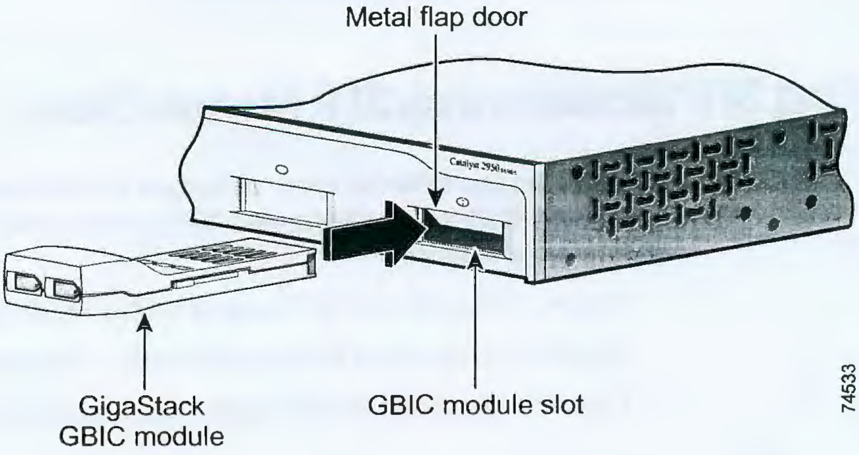


Figure 3-23 Installing a GigaStack GBIC Module in a Switch



Installing and Removing SFP Modules

These sections describe how to install and remove small-form-factor pluggable (SFP) modules. SFP modules are inserted into SFP module slots on the front of the Catalyst 2950 LRE switches. These field-replaceable modules provide the uplink optical interfaces, laser send (TX) and laser receive (RX).

You can use any combination of SFP modules. Refer to the Catalyst 2950 LRE release notes for the list of SFP modules that the Catalyst 2950 LRE switch supports. Each port must match the wave-length specifications on the other end of the cable, and the cable must not exceed the stipulated cable length for reliable communications. Refer to Table 2-2 for cable stipulations for SFP connections.

Use only Cisco SFP modules on the Catalyst 2950 LRE switch. Each SFP module has an internal serial EEPROM that is encoded with security information. This encoding provides a way for Cisco to identify and validate that the SFP module meets the requirements for the switch.

For detailed instructions on installing, removing, and cabling the SFP module, refer to your SFP module documentation.

Installing SFP Modules into SFP Module Slots

SFP modules use different types of latches for their installation and extraction. Determine which type of latch your SFP module uses before following the installation procedure:

- Figure 3-24 shows an SFP module with a Mylar tab latch.
- Figure 3-25 shows an SFP module with an actuator button latch.
- Figure 3-26 shows an SFP module that has a bale-clasp latch.

⚠ **Caution** We strongly recommend that you do not install or remove the SFP module with fiber-optic cables attached to it because of the potential damage to the cables, the cable connector, or the optical interfaces in the SFP module. Disconnect all cables before removing or installing an SFP module.

Removing and installing an SFP module can shorten its useful life. Do not remove and insert SFP modules more often than is absolutely necessary.

Figure 3-24 SFP Module with a Mylar Tab Latch

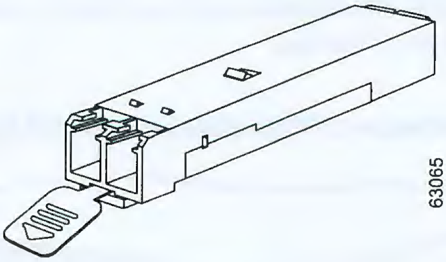


Figure 3-25 SFP Module with an Actuator Button Latch

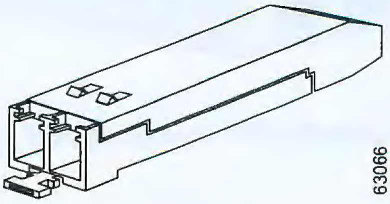
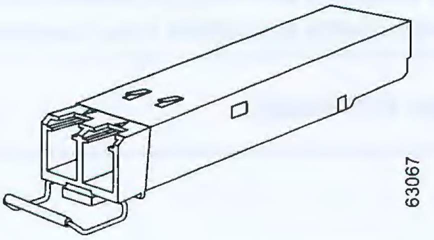


Figure 3-26 SFP Module with a Bale-Clasp Latch



To insert an SFP module into the SFP module slot, follow these steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface on the chassis.

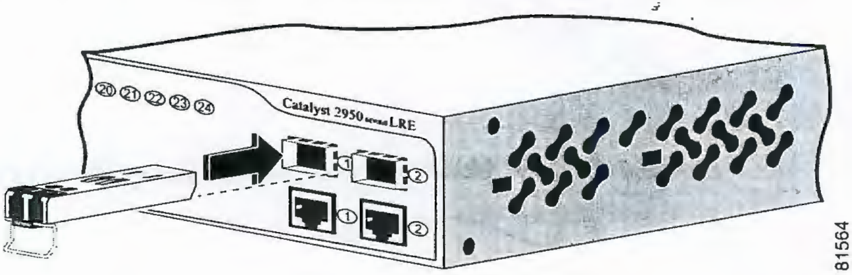
Step 2 Find the send (TX) and receive (RX) markings that identify the top side of the SFP module.

Note On some SFP modules, the send and receive (TX and RX) markings might be replaced by arrows that show the direction of the connection, either send or receive (TX or RX).

Step 3 Align the SFP module in front of the slot opening.

Step 4 Insert the SFP module into the slot until you feel the connector on the module snap into place in the rear of the slot.

Figure 3-27 Installing an SFP Module into an SFP Module Slot



Step 5 Remove the dust plugs from the SFP module optical ports and store them for later use.

Caution Do not remove the dust plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

Step 6 Insert the LC into the SFP module.

Removing SFP Modules from SFP Module Slots

To remove an SFP module from a module receptacle, follow these steps:

Step 1 Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface on the chassis.

Step 2 Disconnect the LC from the SFP module.

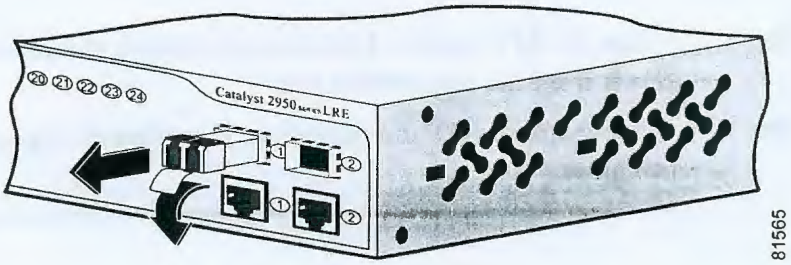
Tip For reattachment, note which cable connector plug is send (TX) and which is receive (RX).

Step 3 Insert a dust plug into the optical ports of the SFP module to keep the optical interfaces clean.

Step 4 Unlock and remove the SFP module, as shown in Figure 3-28, Figure 3-29, and Figure 3-30.

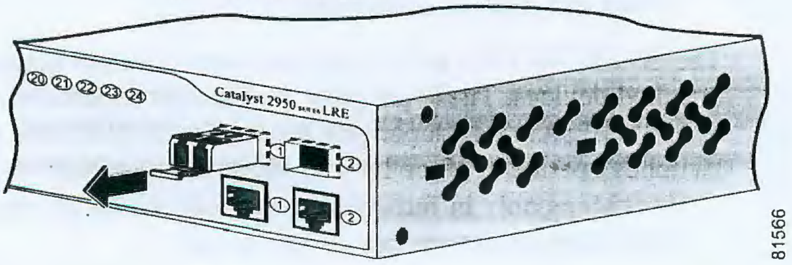
- If the module has a Mylar tab latch, pull the tab straight out so that you remove the SFP module from the port in a parallel direction. Do not twist or pull the tab because you could disconnect it from the SFP module.

Figure 3-28 Using the Mylar Tab Latch to Remove an SFP Module from a Slot



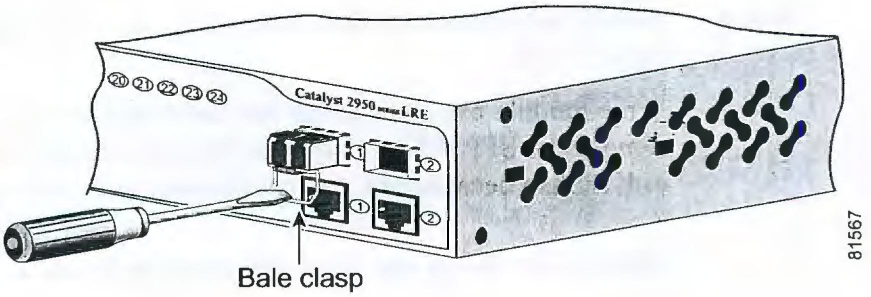
- If the module has an actuator button latch, use your thumb to push inward on the wedge to free the locking pin, and use your index finger to grip the ridge on top of the SFP module. Pull straight out to remove the module.

Figure 3-29 Using the Actuator Button Latch to Remove an SFP Module from an SFP Module Slot



- If the module has a bale-clasp latch, pull the bale out and down to eject the module. If the bale-clasp latch is obstructed and you cannot use your index finger to open it, use a small, flat-blade screwdriver or other long, narrow instrument to open the bale-clasp latch.

Figure 3-30 Removing a Bale-Clasp Latch SFP Module by Using a Flat-Blade Screwdriver



Step 5 Grasp the SFP module between your thumb and index finger, and carefully remove it from the module slot.

Step 6 Place the removed SFP module in an antistatic bag or other protective environment.

Connecting to 10/100 and 10/100/1000 Ports

The 10/100 ports configure themselves to operate at the speed and duplex settings of attached devices.They operate at 10 or 100 Mbps in half- or full-duplex mode. If the attached devices do not support autonegotiation, you can explicitly set the speed and duplex parameters.

The 10/100/1000 ports configure themselves to operate at the speed setting of attached devices. These ports on Catalyst 2950T-24 switches operate at 10, 100, or 1000 Mbps in full-duplex mode. The 10/100/1000 ports on Catalyst 2950 LRE switches operate at 10 or 100 Mbps in either half- or full-duplex mode and at 1000 Mbps only in full-duplex mode. If the attached devices do not support autonegotiation, you can set the speed.

Note On the Catalyst 2950 LRE switches, the four input uplink ports are bundled as two logical ports, each consisting of a copper 10/100/1000 port and a fiber-optic SFP module slot, respectively.

Within each logical port, you can use only the copper or the fiber-optic port at one time. If the Catalyst 2950 LRE switch senses more than two connections for both logical ports, by default, the switch chooses the fiber-optic connections over the copper connections.

See the “SFP Module Slots” section on page 2-14 for more information on LRE uplink logical ports.

Connecting devices that do not autonegotiate or devices with manually set speed and duplex parameters can reduce performance or result in link failures between the devices. To maximize performance, choose one of these methods for configuring the ports:

- Let the 10/100 ports autonegotiate both speed and duplex, let the 10/100/1000 ports on the LRE switches autonegotiate both speed and duplex, and let the 10/100/1000 ports on the Catalyst 2950G-24-EI-DC switch only autonegotiate speed.
- Set the speed and duplex parameters on both ends of the connection.

When connecting the ports on the Catalyst 2950G-24-EI-DC and Catalyst 2950ST-24 LRE 997 switches to other devices, follow these guidelines:

Caution To comply with the intrabuilding lightning surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

Caution The Catalyst 2950G-24-EI-DC or Catalyst 2950ST-24 LRE 997 switch is suitable only for intrabuilding or nonexposed wiring connections.

Follow these steps to connect the switch to 10BASE-T, 100BASE-TX, or 1000BASE-T devices:

Caution To prevent electrostatic-discharge (ESD) damage, follow your normal board and component handling procedures.

Step 1 When connecting to servers, workstations, and routers, insert a twisted-pair straight-through cable in a front-panel RJ-45 connector, as shown in Figure 3-31, Figure 3-32, and Figure 3-33. When connecting to switches or repeaters, insert a twisted-pair crossover cable. (See the "Cable and Adapter Specifications" section on page B-8 for cable-pinout descriptions.)

Note When connecting to 1000BASE-T devices, be sure to use a four twisted-pair, Category 5 cable.

Figure 3-31 Connecting to a Port on Catalyst 2950-12, 2950-24, 2950C-24, 2950SX-24, and 2950T-24 Switches

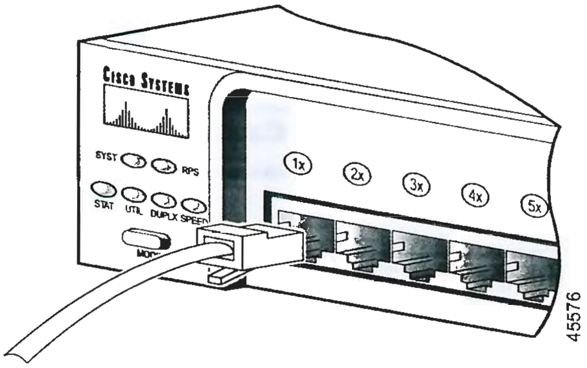


Figure 3-32 Connecting to a Port on Catalyst 2950G-12-EI, 2950G-24-EI, and 2950G-24-EI-DC Switches

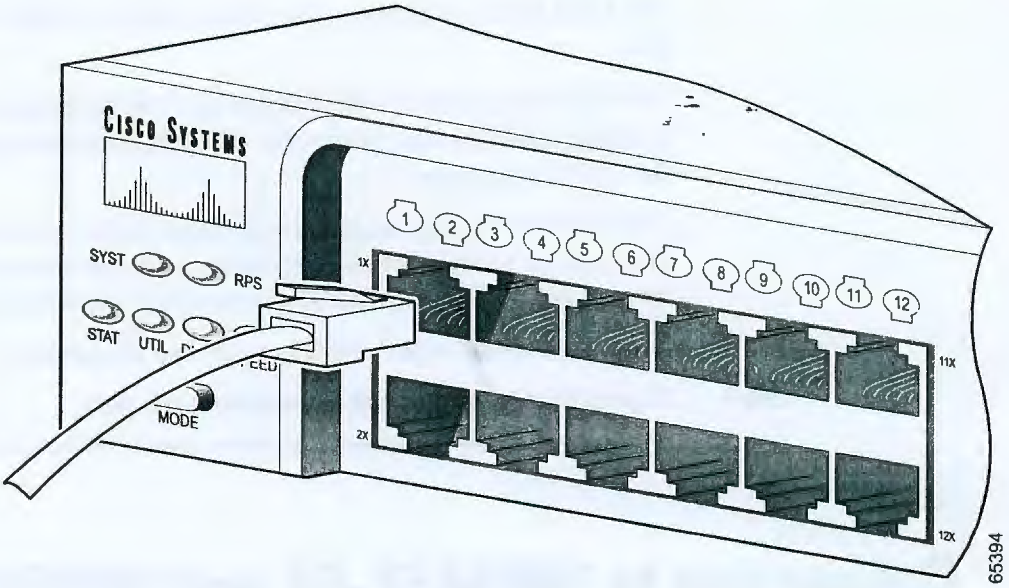
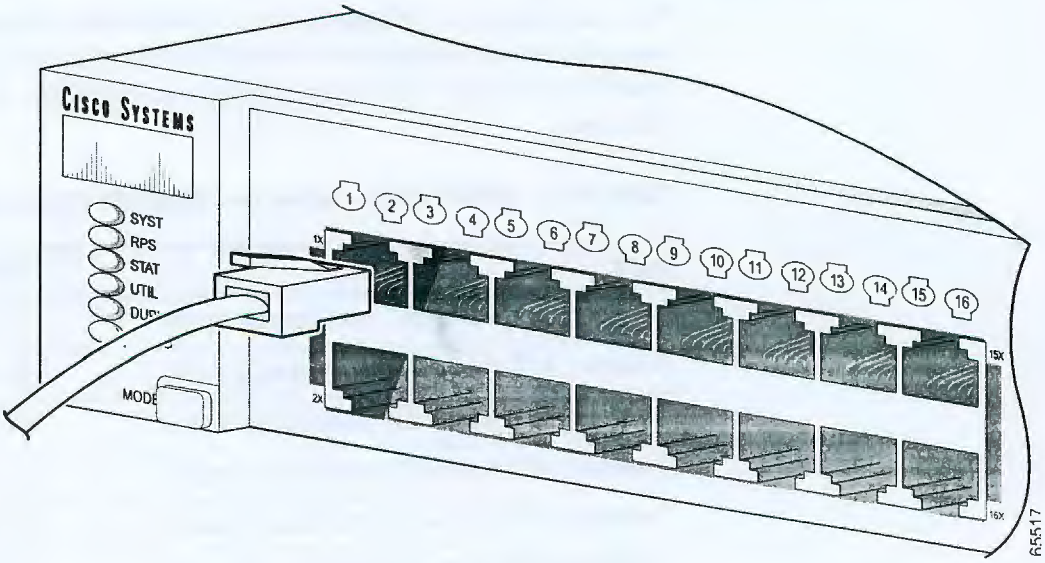


Figure 3-33 Connecting to a Port on Catalyst 2950G-48-EI Switches



Step 2 Insert the other cable end in an RJ-45 connector on the target device.

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while Spanning Tree Protocol (STP) discovers the network topology and searches for loops. This process takes about 30 seconds, and then the LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 4, "Troubleshooting," for solutions to cabling problems.

Step 4 Reconfigure and restart the target device if necessary.

Step 5 Repeat Steps 1 through 4 to connect each port.

Connecting to 100BASE-FX and 1000BASE-SX Ports

The 100BASE-FX and 1000BASE-SX ports operate only in full-duplex mode.

You can connect a 100BASE-FX or 1000BASE-SX port to an SC or ST port on a target device by using one of the MT-RJ fiber-optic patch cables listed in Table 3-1. Use the Cisco part numbers in Table 3-1 to order the patch cables that you need.

Table 3-1 MT-RJ Patch Cables for 100BASE-FX and 1000BASE-SX Connections

Type	Cisco Part Number
1-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-1M
3-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-3M
5-meter, MT-RJ-to-SC multimode cable	CAB-MTRJ-SC-MM-5M
1-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-1M
3-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-3M
5-meter, MT-RJ-to-ST multimode cable	CAB-MTRJ-ST-MM-5M

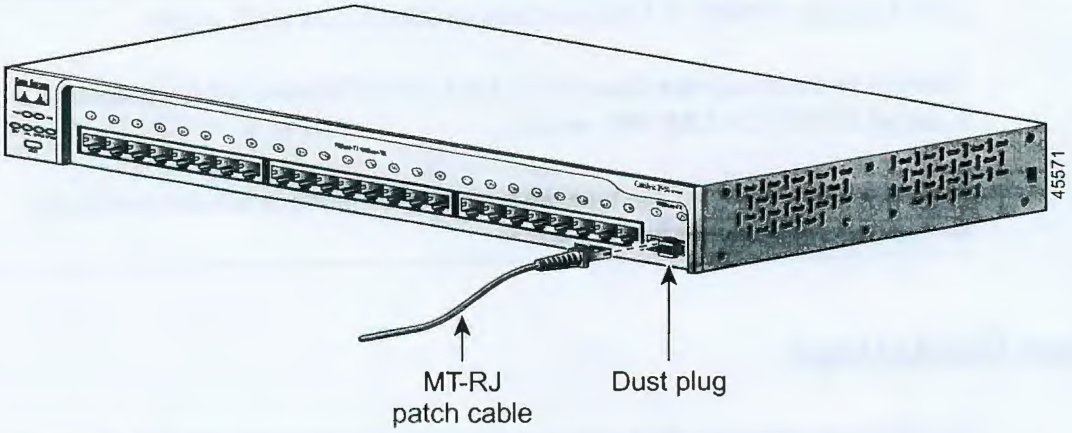
Caution Do not remove the dust plugs from the fiber-optic ports or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the fiber-optic ports and cables from contamination and ambient light.

Follow these steps to connect the switch to a 100BASE-FX or 1000BASE-SX device:

Step 1 Remove the dust plugs from the 100BASE-FX or 1000BASE-SX port and the rubber caps from the MT-RJ patch cable. Store them for future use.

Step 2 Insert the cable in a 100BASE-FX or 1000BASE-SX port. (See Figure 3-34.)

Figure 3-34 Connecting to a 100BASE-FX or 1000BASE-SX Port



Step 3 Insert the other cable end in an SC or ST port on the target device.

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 4, “Troubleshooting,” for solutions to cabling problems.

Step 5 Reconfigure and restart the target device if necessary.

Step 6 Repeat Steps 1 through 5 to connect each port.

Connecting to an LRE Port

Depending on the switch model, you can connect the LRE port to up to 8 or up to 24 LRE customer premises equipment (CPE) devices through a patch panel. For information about which LRE CPE devices are supported by the LRE switches, see Table 2-1 on page 2-4.

Note You can connect both Cisco 575 LRE CPE and Cisco 585 LRE CPE devices to your Catalyst 2950ST-8 LRE or Catalyst 2950ST-24 LRE switch.

You can connect only the Cisco 576 LRE CPE 997 device to LRE ports on a Catalyst 2950ST-24 LRE 997 switch.

You can hot swap the CPE devices without powering down the switch or disrupting the other switch ports.

Connection Guidelines

If telephone services, such as voice or Integrated Services Digital Network (ISDN), use the same cabling as the LRE traffic, you must connect the LRE to a plain old telephone service (POTS) splitter. The splitter routes LRE data (high-frequency) and voice (low-frequency) traffic from the telephone line to the switch and private branch exchange (PBX) switch or public switched telephone network (PSTN).

If the other telephone services are connected through a PBX switch, you can use a Cisco LRE 48 POTS Splitter. The PBX routes voice traffic to private telephone networks and the PSTN. For more information about the Cisco LRE 48 POTS Splitter (PS-1M-LRE-48), refer to the *Installation and Warranty Notes for the Cisco LRE 48 POTS Splitter.*

If the installation does not have a PBX, you need to use a homologated POTS splitter to connect to the PSTN. For more information about homologated POTS splitters, contact your Cisco sales representative.

If a connection to a telephone network is not required, you do not need a splitter, and you can connect the switch to the patch panel.

Limitations and Restrictions with POTS Splitters

These limitations and restrictions apply when you use a POTS splitter with Catalyst 2950 LRE switches and Cisco LRE CPE devices:

- The Catalyst 2950ST-8 LRE switch, Catalyst 2950ST-24 LRE switch, Cisco 575 LRE CPE, and Cisco 585 LRE CPE are designed to share lines with analog, ISDN, and digital PBX switch telephones that use the 0 to 700 kHz frequency range.

  Digital telephones connected to digital PBX switches that use frequencies above 700 kHz do not work when sharing a line with LRE signals. Due to the proprietary nature of digital PBX switches, some digital PBX switch services use frequencies above 700 kHz.

- You can use a Cisco LRE 48 POTS Splitter with a Catalyst 2950ST-8 LRE switch, Catalyst 2950ST-24 LRE switch, Cisco 575 LRE CPE, and Cisco 585 LRE CPE. For installation instructions, refer to the *Installation and Warranty Notes for the Cisco LRE 48 POTS Splitter*.

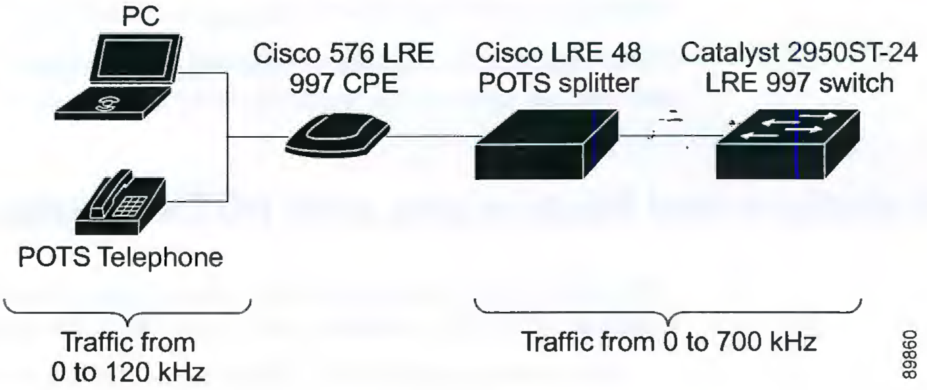
- The Catalyst 2950ST-24 LRE 997 switch and Cisco 576 LRE 997 CPE are designed to share lines with analog and ISDN telephones that use the 0 to 120 kHz frequency range.

- We recommend that *you do not use* a Cisco LRE 48 POTS Splitter with a Catalyst 2950ST-24 LRE 997 switch and a Cisco 576 LRE 997 CPE as shown in Figure 3-35. Only traffic in a specific frequency range can be sent to and from the devices attached to the CPE.

  In Figure 3-35, only traffic from 0 to 120 kHz can pass from a device attached to the CPE, such as a computer or telephone, to the CPE, a splitter, and a switch. In the reverse direction, traffic from 0 to 700 kHz can pass through the switch and splitter to the CPE, but only traffic from 0 to 120 kHz can pass through the CPE to a computer or a telephone.

  For more information, refer to the *Installation and Warranty Notes for the Cisco LRE 48 POTS Splitter*.

Figure 3-35 Limitations Using a Cisco LRE 48 POTS Splitter with a Catalyst 2950ST-24 LRE 997 Switch and a Cisco 576 LRE 997 CPE


PC
Cisco 576 LRE 997 CPE
Cisco LRE 48 POTS splitter
Catalyst 2950ST-24 LRE 997 switch
POTS Telephone
Traffic from 0 to 120 kHz
Traffic from 0 to 700 kHz
89860

Required Cables

Connecting the LRE port to a patch panel or a POTS splitter requires a male-to-male RJ-21 cable, Category 3 or above. You can order RJ-21 cables from your cable vendor, or you can order these cables from your Cisco sales representative:

- CAB-5-M120M120-5= (Category 5 cable with 90-degree, male-to-male RJ-21 connectors)
- CAB-5-M180M120-5= (Category 5 cable with 120-degree, male-to-male RJ-21 connectors)

The screws that you need to secure the cable to the switch are shipped with the cable. Contact your Cisco sales representative for more information.

Connecting to a Patch Panel or POTS Splitter

To connect the LRE port to a patch panel or POTS splitter, follow these steps:

Step 1 Connect one end of a cable connected to the wiring trunk to the RJ-21 connector (the LRE port) on the switch. (See Figure 3-36 and Figure 3-37.)

Step 2 Referring to Figure 3-36 and Figure 3-37, secure the cable to the switch:

- For a 90-degree connector, see the top of Figure 3-36 and Figure 3-37.
- For a 12-degree connector, see the bottom of Figure 3-36 and Figure 3-37.

Note The cable tie is not included with the connector and cable assembly.

Step 3 Connect the other end of the cable to the patch panel or POTS splitter.

Figure 3-36 Connecting to an LRE Port on a Catalyst 2950ST-8 LRE or 2950ST-24 LRE Switch

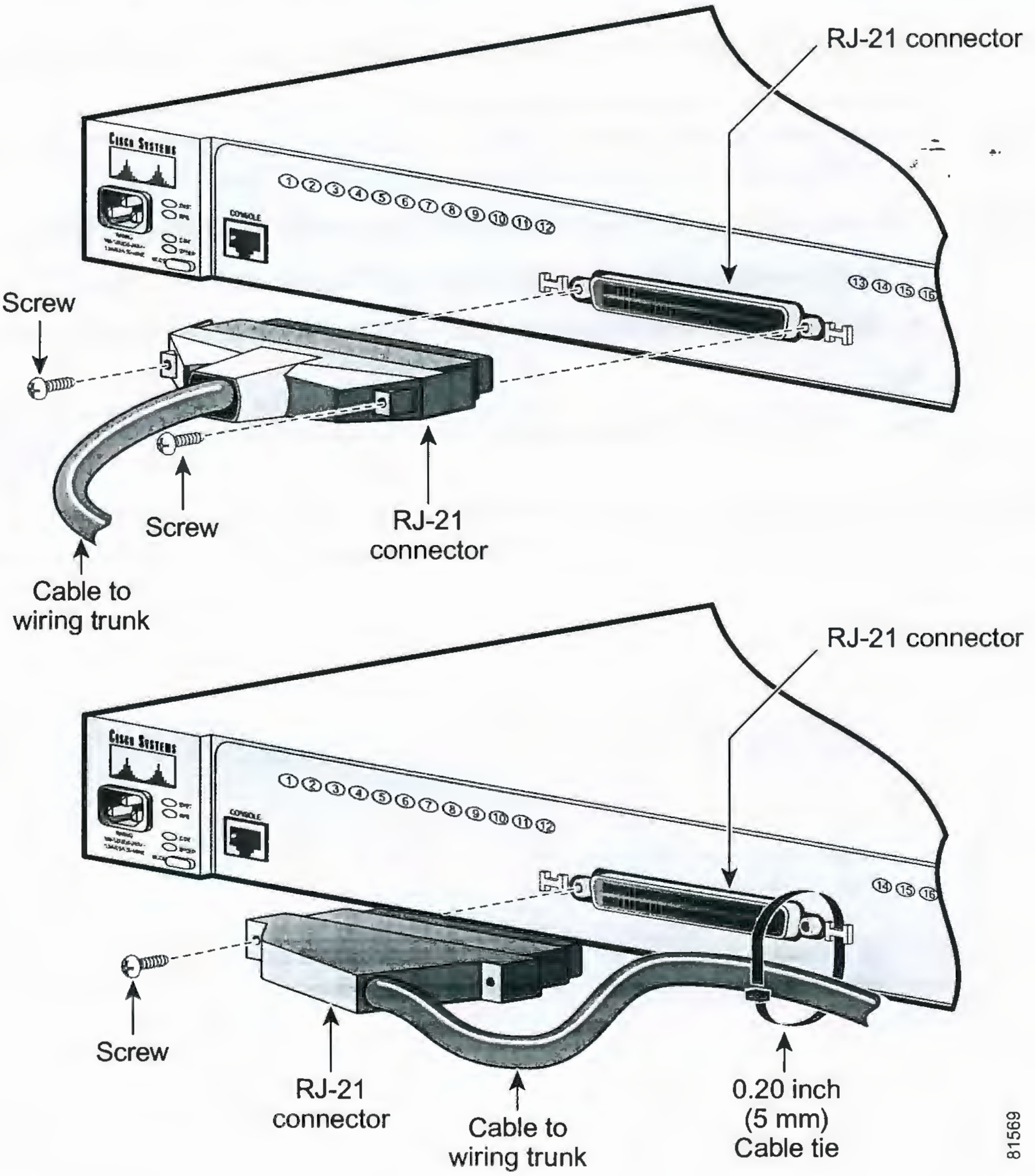
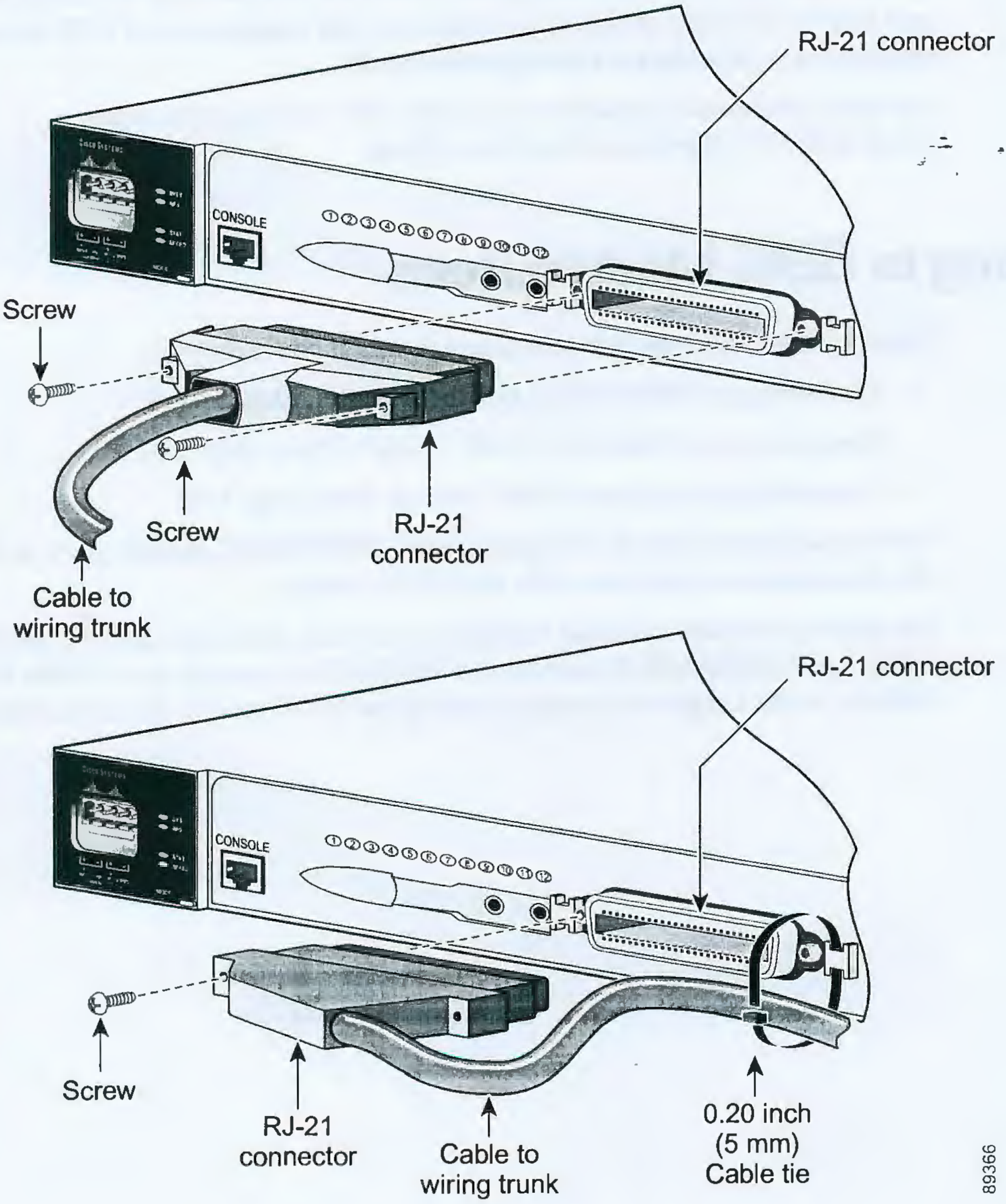


Figure 3-37 Connecting to an LRE Port on a Catalyst 2950ST-24 LRE 997 Switch



Each LRE port status LED turns on when it establishes a link with a Cisco LRE CPE device. For more information about the LRE link between the switch LRE port and the CPE and about the configuration and management of CPE devices, refer to the switch software configuration guide.

For more information about the Cisco LRE CPE devices, refer to the *Cisco LRE CPE Hardware Installation Guide.*

Connecting to GBIC Module Ports

These sections describe how to connect to a GBIC module port.

- Connecting to 1000BASE-X GBIC Module Ports, page 3-45
- Connecting to 1000BASE-T GBIC Module Ports, page 3-47
- Connecting to GigaStack GBIC Module Ports, page 3-48

For instructions about how to connect to the CWDM GBIC module ports, refer to the documentation that came with that GBIC module.

For detailed instructions about installing, removing, and connecting to the GBIC module (the 1000BASE-X module, the 1000BASE-T module, the CWDM GBIC module, or the GigaStack module), refer to the GBIC module documentation.

When connecting the ports on the Catalyst 2950G-24-EI-DC and Catalyst 2950ST-24 LRE 997 switches to other devices, follow these guidelines:

⚠ **Caution** To comply with the intrabuilding lightning surge requirements, intrabuilding wiring must be shielded, and the shield for the wiring must be grounded at both ends.

⚠ **Caution** The Catalyst 2950G-24-EI-DC or Catalyst 2950ST-24 LRE 997 switch is suitable only for intrabuilding or nonexposed wiring connections.

Connecting to 1000BASE-X GBIC Module Ports

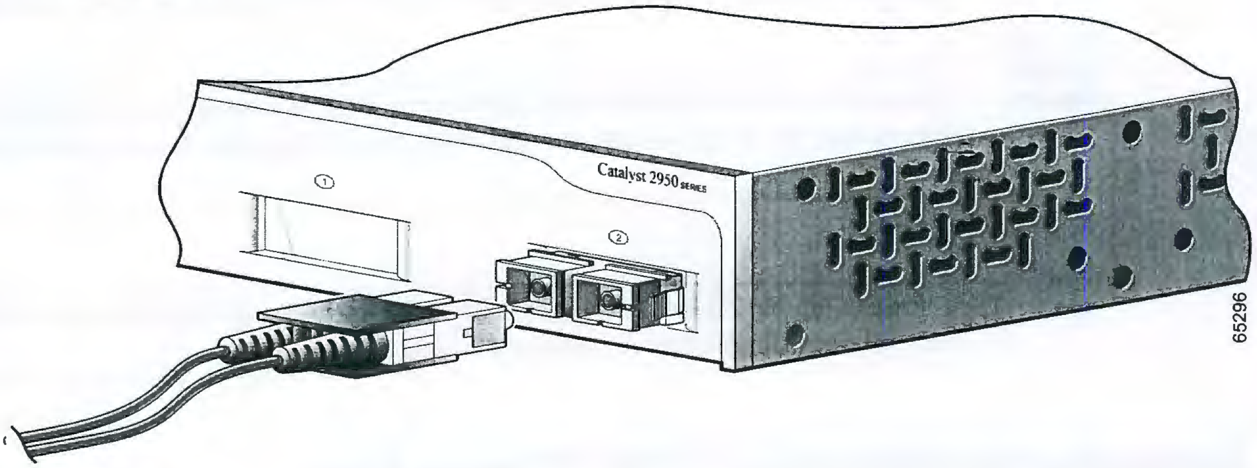
⚠ **Caution** Do not remove the rubber plugs from the GBIC module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the GBIC module ports and cables from contamination and ambient light.

After installing the 1000BASE-X GBIC in the GBIC module slot, follow these steps:

Step 1 Remove the rubber plugs from the GBIC module port, and store them for future use.

Step 2 Insert the SC connector in the fiber-optic receptacle (see Figure 3-38).

Figure 3-38 Connecting to a 1000 BASE-X GBIC Port



Step 3 Insert the other cable end in a fiber-optic receptacle on a target device.

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

Step 5 Reconfigure and restart the switch or target device if necessary.

Connecting to 1000BASE-T GBIC Module Ports

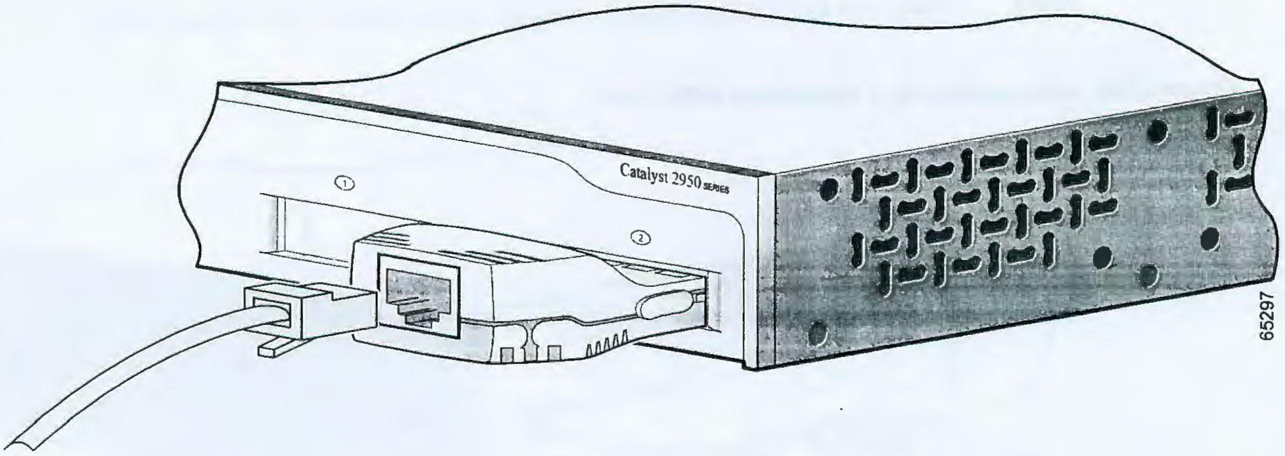
After installing the 1000BASE-T GBIC in the GBIC module slot, follow these steps:

Caution To prevent ESD damage, follow your normal board and component handling procedures.

Step 1 When connecting to servers, workstations, and routers, insert a four twisted-pair, straight-through cable in the RJ-45 connector. When connecting to switches or repeaters, insert a four twisted-pair, crossover cable (see Figure 3-39).

Note When connecting to a 1000BASE-T device, be sure to use a four twisted-pair, Category 5 cable.

Figure 3-39 Connecting to a 1000BASE-T GBIC Port



Step 2 Insert the other cable end in an RJ-45 connector on a target device.

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 3, "Troubleshooting," for solutions to cabling problems.

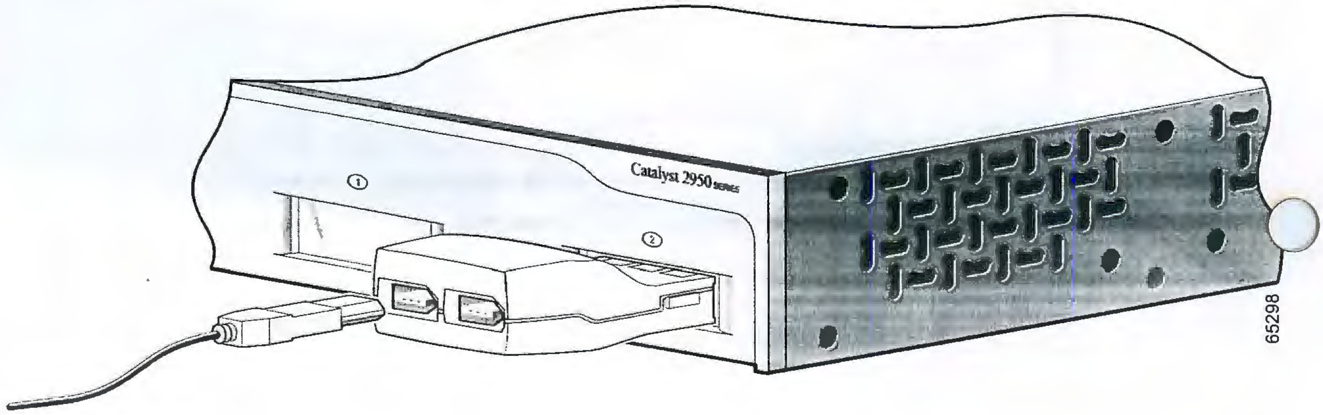
Step 4 Reconfigure and restart the switch or target device, if necessary.

Connecting to GigaStack GBIC Module Ports

After installing the GigaStack GBIC in the GBIC module slot, follow these steps:

Step 1 Insert the GigaStack cable connector in the GBIC (see Figure 3-40).

Figure 3-40 Connecting to a GigaStack GBIC Port



Step 2 Insert the other cable end in a port on a target device.

Step 3 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be a problem with the adapter installed in the target device. See Chapter 4, “Troubleshooting,” for solutions to cabling problems.

Step 4 Reconfigure and restart the switch or target device, if necessary.

Connecting to an SFP Module

This section describes how to connect to an SFP module. For instructions about how to install or remove an SFP module, see the “Installing and Removing SFP Modules” section on page 3-28.

Caution Do not remove the rubber plugs from the SFP module port or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the SFP module ports and cables from contamination and ambient light.

Before connecting to an SFP module, be sure that you understand the port and cabling stipulations in Table 2-2 on page 2-16 and in the “SFP Module Slots” section on page 2-14. See Appendix B, “Connectors and Cables,” for information about the LC on the SFP module.

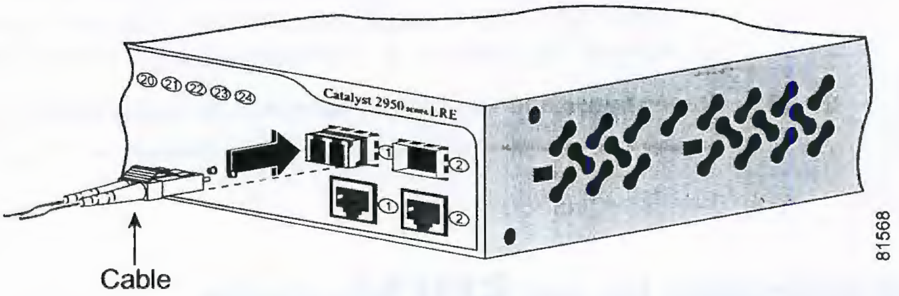
Note Refer to the Catalyst 2950 LRE release notes for the list of supported SFP modules.

Follow these steps to connect a fiber-optic cable to an SFP module:

Step 1 Remove the rubber plugs from the module port and fiber-optic cable, and store them for future use.

Step 2 Insert one end of the fiber-optic cable into the SFP module port (see Figure 3-41).

Figure 3-41 Connecting to an SFP Module Port



Step 3 Insert the other cable end in a fiber-optic receptacle on a target device.

Step 4 Observe the port status LED.

The LED turns green when the switch and the target device have an established link.

The LED turns amber while the STP discovers the network topology and searches for loops. This process takes about 30 seconds, and then the port LED turns green.

If the LED is off, the target device might not be turned on, there might be a cable problem, or there might be problem with the adapter installed in the target device. See Chapter 3, “Troubleshooting,” for solutions to cabling problems.

Step 5 If necessary, reconfigure and restart the switch or target device.

Where to Go Next

For information about starting up the switch, see Chapter 1, “Quick Installation.”

For information about configuring the switch, refer to the switch software configuration guide.

Apêndice FM

CISCO SYSTEMS

Data Sheet

Cisco Catalyst 2950 Series Switches with Cisco **Enhanced** Image Software

Product Overview

Cisco® Catalyst® 2950 Series switches are fixed-configuration, stackable models that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity for small and medium-sized networks. The Cisco Catalyst 2950 Series is an affordable product line that brings intelligent services, such as enhanced security, high availability and advanced quality of service (QoS), to the network edge—while maintaining the simplicity of traditional LAN switching. When a Cisco Catalyst 2950 Series Switch is combined with a Cisco Catalyst 3550 Series Switch, the solution can enable IP routing from the edge to the core of the network. Embedded in Cisco Catalyst 2950 Series switches is Cisco Cluster Management Suite (CMS) Software, which allows users to simultaneously configure and troubleshoot multiple Cisco Catalyst desktop switches using a standard Web browser. In addition to Cisco CMS Software, Cisco Catalyst 2950 Series switches provide extensive management tools using Simple Network Management Protocol (SNMP) network management platforms such as CiscoWorks.

This product line offers two distinct sets of software features and several configurations to allow small, medium-sized, and enterprise branch offices to select the right combination for the network edge. Cisco Standard Image (SI) Software offers Cisco IOS® Software functioning for basic data, video, and voice services. For networks with requirements for additional security, advanced QoS, and high availability, the Cisco Enhanced Image (EI) Software delivers intelligent services such as rate limiting and security filtering for deployment at the network edge.

The Cisco Catalyst 2950 Series switches consists of the following devices—which are only available with Cisco EI Software for the Cisco Catalyst 2950 Series.

- Catalyst 2950G-48—48 10/100 ports and 2 Gigabit Interface Converter (GBIC)-based Gigabit Ethernet ports
- Catalyst 2950G-24—24 10/100 ports and 2 GBIC ports
- Catalyst 2950G-24-DC—24 10/100 ports, 2 GBIC ports, and DC power
- Catalyst 2950G-12—12 10/100 ports and 2 GBIC ports
- Catalyst 2950T-24—24 10/100 ports and 2 fixed 10/100/1000BASE-T uplink ports
- Catalyst 2950C-24—24 10/100 ports and 2 fixed 100BASE-FX uplink ports

This complete set of switches offers network managers flexibility when selecting a migration path to Gigabit Ethernet. The two built-in Gigabit Ethernet ports on the Cisco Catalyst 2950G-12, 2950G-24, and 2950G-48 accommodate a range of GBIC transceivers, including the Cisco GigaStack® GBIC, as well as 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, 1000BASE-T, and coarse-wave division multiplexing (CWDM) GBICs. The dual GBIC-based Gigabit Ethernet implementation provides customers with tremendous deployment flexibility—allowing customers increased availability with the redundant uplinks. In sum, the configuration permits customers to implement one type of stacking and uplink configuration today, while preserving the option to migrate to another configuration in the future. High levels of stack resiliency can also be implemented by deploying dual-redundant Gigabit Ethernet uplinks, a redundant GigaStack GBIC loopback cable, Cisco UplinkFast and CrossStack UplinkFast technologies for high-speed uplink and stack interconnection failover, and Per-VLAN Spanning Tree Plus (PVST+) for uplink load balancing.

The Cisco Catalyst 2950T-24 Switch offers small and medium-sized enterprises server connectivity and an easy migration path to Gigabit by using the existing copper cabling infrastructure. Implementing Gigabit Ethernet over copper allows network managers to boost network performance and maximize infrastructure investments in Category 5 copper cabling.

Maximum power availability for a converged voice and data network is attainable when a Cisco Catalyst 2950 Se Switch is combined with the Cisco Redundant Power System (RPS) 300 or RPS 675 for protection against interna power supply failures and an uninterruptable power supply (UPS) system to safeguard against power outages.

Other Cisco Catalyst 2950 Series Switches

Cisco Catalyst 2950 Series with Cisco SI Software

The Cisco Catalyst 2950SX-24, 2950-24, and 2950-12 switches are also members of the Cisco Catalyst 2950 Series. They are standalone, fixed-configuration, and managed 10/100 switches providing basic workgroup connectivity for small to medium-sized companies. These wire-speed desktop switches come with Cisco SI Software features and offer Cisco IOS Software functioning for basic data, video, and voice services at the edge of the network.

Cisco Catalyst 2950 Series Long-Reach Ethernet Switches

- *Cisco Catalyst 2950ST-24-LRE*—24 long-reach Ethernet (LRE) ports, 2 fixed 10/100/1000BASE-T ports, and two small form factor pluggable (SFP) ports (2 of the 4 uplinks active at one time)
- *Cisco Catalyst 2950ST-8-LRE*—Eight LRE ports, 2 fixed 10/100/1000BASE-T ports, and two SFP ports (two of the four uplinks active at one time)

The Cisco Catalyst 2950 Series LRE switch solution delivers cost-effective, high-performance broadband access over existing phone wiring in enterprise campus environments and multitenant buildings (hotels, apartment buildings, office buildings, for example). Cisco Catalyst 2950 Series LRE switches come with Cisco EI Software features, enabling enterprise and service provider customers to extend intelligent services over legacy wiring (Category 1, 2, and 3) to distances up to 5000 feet. Cisco is the only company with technologies that allow customers to deliver intelligent network services across any combination of wired and wireless infrastructures. Refer to the Cisco Catalyst 2950 Series LRE Data Sheet for more information.

Intelligence in the Network

Networks are evolving to address four new developments at the network edge:

- Increase in desktop computing power
- Introduction of bandwidth-intensive applications
- Expansion of highly sensitive data on the network
- Presence of multiple device types, such as IP phones and wireless LAN (WLAN) access points

These new demands are contending for resources with many existing mission-critical applications. As a result, IT professionals must view the edge of the network as critical to the effective management of the delivery of information and applications.

As companies increasingly rely on networks as the strategic business infrastructure, it is more important than ever to ensure high availability, security, scalability, and control. By adding Cisco intelligent functioning to the wiring closet, customers can now deploy network-wide intelligent services that address these requirements in a consistent way, from the desktop to the core and through the WAN.

With Cisco Catalyst switches, Cisco enables companies to fully realize the benefits of adding intelligent services into their networks. Making the network infrastructure highly available to accommodate time-critical needs, scalable to accommodate growth, secure enough to protect confidential information, and capable of differentiating and controlling traffic flows is critical to further optimizing network operations.

Network Security Through Advanced Security Features

Cisco Catalyst 2950 Series switches offer enhanced data security through numerous security features. These features allow customers to enhance LAN security with capabilities to secure network management traffic through the protection of passwords and configuration information; to provide options for network security based on users, ports, and Media Access Control (MAC) addresses; and to enable more immediate reactions to intruder and hacker detection. These security enhancements are available free of charge by downloading the latest software release for the Cisco Catalyst 3550 and 2950 series switches.

Secure Shell (SSH) and SNMPv3 protect information from tampering or eavesdropping by encrypting information being passed along the network, guarding administrative information. Private VLAN Edge isolates ports on a switch, ensuring that traffic travels directly from the entry point to the aggregation device through a virtual path and that it cannot be directed to another port. Local Proxy Address Resolution Protocol (ARP) works in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth.

Port-based access control parameters (ACPs) restrict sensitive portions of the network by denying packets based on source and destination MAC addresses, IP addresses, or Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports. ACP lookups are performed in hardware; therefore, forwarding performance is not compromised when implementing this type of security in the network. In addition, time-based access control lists (ACLs) allow configuration of differentiated services based on time periods. ACLs can also be applied to filter traffic based on Differentiated Services Code Point (DSCP) values. Port security provides another means to ensure the appropriate user is on the network by limiting access based on MAC addresses.

For authentication of users with a Terminal Access Controller Access Control System (TACACS+) or Remote Authentication Dial-In User Service (RADIUS) server, 802.1x provides port-level security. In conjunction with a RADIUS server, 802.1x allows for dynamic port-based user authentication, which can be extended to dynamically assign a virtual LAN (VLAN) based on a specific user, regardless of where they connect on the network. This intelligent adaptability allows IT departments to offer greater flexibility and mobility to their stratified user populations. By combining access control and user profiles with secure network connectivity, services, and applications, enterprises can more effectively manage user mobility and drastically reduce the overhead associated with granting and managing access to network resources.

With multilayer Cisco Catalyst 2950 Series switches, network managers can implement high levels of console security. Multilevel access security on the switch console and the Web-based management interface prevent unauthorized users from accessing or altering switch configuration. TACACS+ or RADIUS authentication enables centralized access control of the switch and restricts unauthorized users from altering the configuration. Deploying security can be done through Cisco CMS Software security wizards, which ease the deployment of security features that restrict user access to a server, a portion of the network, or the entire network.

Network Control Through Advanced QoS and Rate Limiting

Cisco Catalyst 2950 Series switches offer superior and highly granular QoS based on Layer 2–4 information to ensure that network traffic is classified and prioritized, and that congestion is avoided in the best possible manner. Configuration of QoS is greatly simplified through automatic QoS (auto-QoS), a feature that detects Cisco IP phones and automatically configures switches for the appropriate classification and egress queuing. This optimizes traffic prioritization and network availability without the challenge of a complex configuration.

Cisco Catalyst 2950 Series switches can classify, reclassify, police (determine if the packet is in or out of predetermined profiles and affect actions on the packet), and mark or drop the incoming packets before the packet is placed in the shared buffer. Packet classification allows the network elements to discriminate between various traffic flows and enforce policies based on Layer 2 and Layer 3 QoS fields.

To implement QoS, these switches first identify traffic flows (or packet groups) and classify or reclassify these groups using the DSCP field in the IP packet or the 802.1p class of service (CoS) field in the Ethernet packet. Classification and reclassification can also be based on criteria as specific as the source/destination IP address, source/destination MAC address, or the Layer 4 TCP/UDP ports. At the ingress (incoming port) level, the Cisco Catalyst switches will also perform policing and marking of the packet.

After the packet goes through classification, policing, and marking, it is assigned to the appropriate queue before exiting the switch. Cisco Catalyst 2950 Series switches support four egress (outgoing port) queues per port, which allows the network administrator to be more discriminating and specific in assigning priorities for the various applications on the LAN. At the egress level, the switch performs scheduling, which is a process that determines the order in which the queues are processed. The switches support Weighted Round Robin (WRR) scheduling or strict priority scheduling. The WRR scheduling algorithm ensures that lower priority packets are not entirely starved for bandwidth and are serviced without compromising the priority settings administered by the network manager. Strict priority scheduling ensures that the highest priority packets will always get serviced first, ahead of all other traffic, and that the other three queues will be serviced using WRR best effort.

These features allow network administrators to prioritize mission-critical or bandwidth-intensive traffic, such as enterprise resource planning (ERP) (Oracle, SAP, and so on), voice (IP telephony traffic), and CAD/CAM over less time-sensitive applications such as File Transfer Protocol (FTP) or e-mail (SMTP). For example, it would be highly undesirable to have a large file download destined to one port on a wiring closet switch and have quality implications, such as increased latency in voice traffic, destined to another port on this switch. This condition is avoided by ensuring that voice traffic is properly classified and prioritized throughout the network. Other applications, such as Web browsing, can be treated as low priority and handled on a best-effort basis.

Cisco Catalyst 2950 Series switches are capable of allocating bandwidth based on several criteria, including MAC source address, MAC destination address, IP source address, IP destination address, and TCP/UDP port number. Bandwidth allocation is essential in network environments that require service-level agreements, or when it is necessary for the network manager to control the bandwidth given to certain users. Cisco Catalyst 2950 Series switches support up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port, giving the network administrator granular control of LAN bandwidth.

Network Availability

To provide efficient use of resources for bandwidth-hungry applications like multicasts, Cisco Catalyst 2950 Series switches support Internet Group Management Protocol (IGMP) snooping in hardware. Through the support and configuration of IGMP snooping via Cisco CMS Software, Cisco Catalyst 2950 Series switches deliver outstanding performance and ease of use in administering and managing multicast applications on the LAN.

The IGMP snooping feature allows the switch to "listen in on" the IGMP conversation between hosts and routers. When a switch hears an "IGMP join" request from a host for a given multicast group, the switch adds the host's port number to the group destination address (GDA) list for that group. When the switch hears an "IGMP leave" request, it removes the host's port from the content-addressable memory (CAM) [CAM ACRONYM IS USED TWICE IN DIFFERENT CONTEXTS] table entry.

PVST+ allows users to implement redundant uplinks while distributing traffic loads across multiple links. This is not possible with standard Spanning-Tree Protocol implementations. Cisco UplinkFast technology helps ensure immediate transfer to the secondary uplink, an improvement over the traditional 30-to-60 second convergence time. An additional feature that enhances performance is Voice VLAN, which allows network administrators to assign voice traffic to a VLAN dedicated to IP telephony—simplifying phone installations and providing easier network traffic administration and troubleshooting.

Multicast VLAN Registration (MVR) is designed for applications that use wide-scale deployment of multicast traffic across an Ethernet-ring-based service provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN.

Network Management

Cisco CMS Software is Web-based and embedded in Cisco Catalyst 3550, 2950, 3500 XL, 2900 XL, and 2900 LRE XL series switches. Through Cisco switch clustering technology, users can access Cisco CMS Software with any standard Web browser to manage up to 16 of these switches at once, regardless of their geographic proximity—with the option of using a single IP address for the entire cluster if desired. With the addition of the Cisco Catalyst 3550 Series switches, Cisco CMS Software can now extend beyond routed boundaries for even more flexibility in managing a Cisco cluster.

Cisco CMS Software provides an integrated management interface for delivering intelligent services, such as multilayer switching, QoS, multicast, and security ACLs. Cisco CMS Software allows administrators to take advantage of benefits formerly reserved for only the most advanced networks without having to learn the command-line interface (CLI) or even the details of the technology.

The new Guide Mode in Cisco CMS Software leads the user step-by-step through the configuration of advanced features and provides enhanced online help for context-sensitive assistance. In addition, Cisco AVVID (Architecture for Voice, Video and Integrated Data) wizards provide automated configuration of the switch to optimally support video streaming or videoconferencing, voice over IP (VoIP), and mission-critical applications. These wizards can save hours of time for network administrators, eliminate human errors, and help ensure that the configuration of the switch is optimized for these applications.

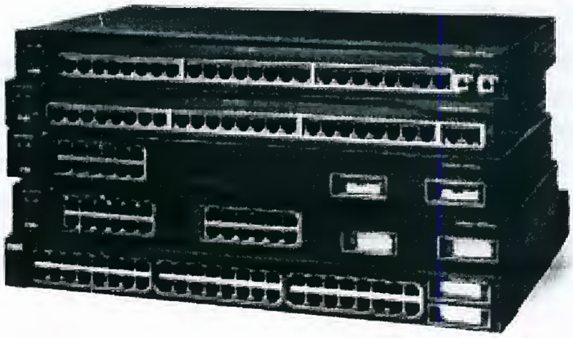
Cisco CMS Software supports standards-based connectivity options such as Ethernet, Fast Ethernet, Fast EtherChannel, Gigabit Ethernet, and Gigabit EtherChannel connectivity. Because Cisco switch clustering technology is not limited to a single stack of switches, Cisco CMS Software expands the traditional cluster domain beyond single wiring closet and saves time and effort for network administrators.

Cisco Catalyst 2950 Series switches can be configured either as command or member switches in a Cisco switch cluster. Cisco CMS Software also allows the network administrator to designate a standby or redundant command switch, which takes the commander duties should the primary command switch fail. Other features include the ability to configure multiple ports and switches simultaneously, to perform software updates across the entire cluster at once, and to clone configurations to other clustered switches for rapid network deployment. Bandwidth graphs and link reports provide useful diagnostic information, and the topology map gives network administrators a quick view of the network status.

In addition to Cisco CMS Software, Cisco Catalyst 2950 Series switches provide extensive management tools using SNMP network management platforms such as CiscoWorks for switched internetworks.

Cisco Catalyst 2950 Series switches deliver a comprehensive set of management tools to provide the required visibility and control in the network (Figure 1). Managed with CiscoWorks, Cisco Catalyst switches can be configured and managed to deliver end-to-end device, VLAN, traffic, and policy management. Coupled with CiscoWorks, Cisco Resource Manager Essentials, a Web-based management tool, offers automated inventory collection, software deployment, easy tracking of network changes, views into device availability, and quick isolation of error conditions.

Figure 1
Cisco Catalyst 2950 Series Switches



Product Features and Benefits

Table 1 lists the features and benefits of the Cisco Catalyst 2950 Series switches.

Table 1 Features and Benefits

Feature	Benefit
Availability	
Superior redundancy for fault backup	• IEEE 802.1D Spanning-Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • Support for Cisco Spanning-Tree Protocol enhancements such as UplinkFast, BackboneFast, and PortFast technologies ensure quick failover recovery, enhancing overall network stability and availability. • IEEE 802.1w Rapid Spanning-Tree Protocol (RSTP) provides rapid convergence of the spanning tree independent of spanning-tree timers. • Cisco CrossStack UplinkFast technology extends UplinkFast to a stack to ensure quick failover recovery, enhancing network stability and availability. • Support for the optional 300-watt or 675-watt redundant Cisco AC power system provides a backup power source for up to 4 or 6 units, respectively, for improved fault tolerance and network uptime. • Redundant stacking connections provide support for a redundant loopback connection for top and bottom switches in an independent stack backplane cascaded configuration. • Command switch redundancy enabled in Cisco CMS Software allows customers to designate a backup command switch that takes over cluster management functions if the primary command switch fails. • Unidirectional link detection (UDLD) and aggressive UDLD features detect and disable unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults.
Integrated Cisco IOS Software features for bandwidth optimization	• Bandwidth aggregation of up to 4 Gbps (2 ports full duplex) through Cisco Gigabit EtherChannel® technology and up to 16 Gbps (8 ports full duplex) through Fast EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches, to routers and individual servers. Port Aggregation Protocol (PAgP) is available to simplify configuration. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance. • PVST+ allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. • IEEE 802.1s Multiple Spanning-Tree Protocol (MSTP) allows a spanning tree instance per VLAN, enabling Layer 2 load sharing on redundant links. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices. Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports in the switch. • IGMP snooping provides for fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors. MVR, IGMP filtering, fast-join, and immediate leave are available as enhancements. • MVR continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons. • Supports additional frame formats: Ethernet II (tagged and untagged), 802.3 (sequence number protection [SNAP] encapsulated tagged and untagged frames)

Feature	Benefit
Security	
Network-wide security features	• Filtering of incoming traffic flows based on Layer 2–4 ACPs prevents unauthorized data flows. – The following Layer 2 ACPs (or a combination) can be used for security classification of incoming packets: source MAC address, destination MAC address, and 16-bit Ethertype. – The following Layer 3 and Layer 4 fields (or a combination) can be used for security classification of incoming packets: source IP address, destination IP address, TCP source or destination port number, UDP source, or destination port number. ACLs can also be applied to filter based on DSCP values. – Time-based ACLs allow configuration of differentiated services based on time periods. • A private VLAN edge provides security and isolation between ports on a switch, helping to ensure that voice traffic travels directly from its entry point to the aggregation device through a virtual path and that it cannot be directed to a different port. • Support for the 802.1x standard allows users to be authenticated, regardless of which LAN port they are accessing, and provides unique benefits to customers who have a large base of mobile (wireless) users accessing the network. . 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user, regardless of where the user is connected. . 802.1x with an ACL assignment allows for specific security policies based on a user, regardless of where the user is connected. . 802.1x with Voice VLAN gives an IP phone access to the Voice VLAN regardless of the authorized or unauthorized state of the port. • 802.1x with port security enables authenticating the port and managing network access for all MAC addresses, including that of the client. • SSH and SNMPv3 provides network security by encrypting administrator traffic during Telnet and SNMP sessions. SSH and the crypto version of SNMPv3 require a special crypto software image due to U.S. export restrictions. • Port Security secures the access to a port based on the MAC address of a user's device. The aging feature removes the MAC address from the switch after a specific timeframe to allow another device to connect to the same port. • MAC Address Notification allows administrators to be notified of new users added or removed from the network. • Spanning-tree root guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning-Tree Protocol root nodes. • The Spanning-Tree Protocol PortFast/bridge protocol data unit (BPDU) guard feature disables access ports with Spanning-Tree Protocol PortFast-enabled upon reception of a BPDU, and increases network reliability, manageability, and security. • Multilevel security on console access prevents unauthorized users from altering the switch configuration. • TACACS+ and RADIUS authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration. • The user-selectable address-learning mode simplifies configuration and enhances security. • Trusted Boundary provides the ability to trust the QoS priority settings if an IP phone is present and to disable the trust setting in the event that the IP phone is removed, preventing a rogue user from overriding prioritization policies in the network. • IGMP Filtering provides multicast authentication by filtering out nonsubscribers and limiting the number of concurrent multicast streams available per port. • Support for dynamic VLAN assignment through implementation of the VLAN Membership Policy Server (VMPS) client function provides flexibility in assigning ports to VLANs. Dynamic VLAN enables fast assignment of IP addresses. • Cisco CMS Software security wizards ease the deployment of security features for restricting user access to a server, a portion of the network, or the entire network.

Feature	Benefit
QoS	
Overview	• The switches support the aggregate QoS model by enabling classification, policing/ metering, and marking functions on a per-port basis at ingress and the queuing/ scheduling function at egress. • The switches support configuring QoS ACPs on all ports to ensure proper policing and marking on a per-packet basis using ACPs. Up to 4 ACPs per switch are supported in configuring either QoS ACPs or security filters. • Auto-QoS greatly simplifies the configuration of QoS in VoIP networks by issuing interface and global switch commands that allow the detection of Cisco IP phones, the classification of traffic, and egress queue configuration.
Qos classification support at ingress	• The switches support QoS classification of incoming packets for QoS flows based on Layer 2–4 fields. • The following Layer 2 fields (or a combination) can be used for classifying incoming packets to define QoS flows: source MAC address, destination MAC address, and 16-bit Ethertype. • The switches support identification of traffic based on Layer 3 type of service (ToS) field and DSCP values. • The following Layer 3 and 4 fields (or a combination) can be used to classify incoming packets to define QoS flows: source IP address, destination IP address, TCP source or destination port number, and UDP source or destination port number.
Qos metering/ policing at ingress	• Support for metering/policing of incoming packets restricts incoming traffic flows to a certain rate. • The switches support up to 6 policers per Fast Ethernet port, and 60 policers on a Gigabit Ethernet port. • The switches offer granularity of traffic flows at 1 Mbps on Fast Ethernet ports, and 8 Mbps on Gigabit Ethernet ports.
Qos marking at ingress	• The switches support marking/remarking packets based on state of policers/meters. • The switches support marking/remarking based on the following mappings: from DSCP to 802.1p, and from 802.1p to DSCP. • The switches support 14 widely used DSCP values. • The switches support classifying or reclassifying packets based on default DSCP per port. They also support classification based on DSCP values in the ACL. • The switches support classifying or reclassifying frames based on the default 802.1p value per port. • The switches support 802.1p override at ingress.
QoS scheduling support at egress	• 4 queues per egress port are supported in hardware. • The WRR queuing algorithm ensures that low-priority queues are not starved. • Strict-priority queue configuration via Strict Priority Scheduling ensures that time-sensitive applications such as voice always follow an expedited path through the switch fabric.
Sophisticated traffic management	• The switch supports up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port. • The switch offers granularity of traffic flows at 1 Mbps on Fast Ethernet ports and 8 Mbps on Gigabit Ethernet ports. • The switch offers the ability to limit data flows based on MAC source/destination address, IP source/destination address, TCP/UDP port numbers, or any combination of these fields. • The switch offers the ability to manage data flows asynchronously upstream and downstream from the end station or on the uplink.

Feature	Benefit
Management	
Superior manageability	• An embedded Remote Monitoring (RMON) software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • The switch supports all 9 RMON groups through the use of a Cisco SwitchProbe® Analyzer (Switched Port Analyzer [SPAN]) port, permitting traffic monitoring of a single port, a group of ports, or the entire switch from a single network analyzer or RMON probe. • A SPAN port monitors traffic of a single port from a single network analyzer or RMON probe. • Remote Switch Port Analyzer (RSPAN) allows network administrators to locally monitor ports in a Layer 2 switch network from any other switch in the same network. • The Domain Name System (DNS) provides IP address resolution with user-defined device names. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all switches within the intranet. • Layer 2 Traceroute eases troubleshooting by identifying the physical path that a packet takes from the source device to a destination device. • Crash Information Support enables a switch to generate a crash file for improved troubleshooting. • Show-interface-capabilities provides information on configuration capabilities of any interface. • The RTTMON [EXPAND?] Management Information Base (MIB) allows users to monitor network performance between a Cisco Catalyst switch and a remote device. • Multifunction LEDs per port for port status, half-duplex/full-duplex, 10BASE-T/100BASE-TX/1000BASE-T indication, as well as switch-level status LEDs for system, redundant power supply, and bandwidth utilization, provide a comprehensive and convenient visual management system.
Management	

Feature	Benefit
Cisco CMS Software	• Cisco CMS Software allows the user to manage up to 16 interconnected Cisco Catalyst 3550, 2950, 3500 XL, 2900 XL, and 2900 LRE XL series switches without the limitation of being physically located in the same wiring closet, and with the option of using a single IP address for the entire cluster if desired. Full backward compatibility helps ensure that any combination of the above switches can be managed with a Cisco Catalyst 2950 Series switch. • Cisco AVVID wizards use just a few user inputs to automatically configure the switch to optimally handle different types of traffic—voice, video, multicast, or high-priority data. • A security wizard is provided to restrict unauthorized access to servers and networks, and to restrict certain applications on the network. • One-click software upgrades can be performed across the entire cluster simultaneously, and configuration cloning enables rapid deployment of networks. • Cisco CMS Software has been extended to include multilayer feature configurations such as ACPs and QoS parameters. • Cisco CMS Software Guide Mode assists users in the configuration of powerful advanced features by providing step-by-step instructions. • Cisco CMS Software provides enhanced online help for context-sensitive assistance. • An easy-to-use graphical interface provides both a topology map and a front-panel view of the cluster. • Multidevice and multiport configuration capabilities allow network administrators to save time by configuring features across multiple switches and ports simultaneously. • Ability to launch the Web-based management for a Cisco Aironet® Wireless Access Point by simply clicking on its icon in the topology map. • A user-personalized interface allows users to modify polling intervals, table views, and other settings within Cisco CMS Software and to retain these settings the next time they use the software. • Alarm notification provides automated e-mail notification of network errors and alarm thresholds.
Support for CiscoWorks	• Manageable through CiscoWorks network management software on a per-port and per-switch basis provides a common management interface for Cisco routers, switches, and hubs. • SNMP v1, v2, and v3 (non-crypto) and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management. • Cisco Discovery Protocol Versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Supported by the CiscoWorks LAN Management Solution.
Management	

Feature	Benefit
Ease of use and ease of deployment	• The Cisco GigaStack® GBIC delivers a hardware-based, independent stacking bus with up to a 2-Gbps forwarding rate in a point-to-point configuration, or 1 Gbps of forwarding bandwidth when daisy-chained [OKAY TERM?] with up to 9 switches. • Autoconfiguration eases the deployment of switches in the network by automatically configuring multiple switches across a network via a boot [P?] server. • Auto-QoS greatly simplifies the configuration of QoS in VoIP networks by issuing interface and global switch commands that allow the detection of Cisco IP phones, the classification of traffic, and egress queue configuration. • Autosensing on each non-GBIC port detects the speed of the attached device and automatically configures the port for 10-, 100-, or 1000-Mbps operation, easing the deployment of the switch in mixed 10, 100, and 1000BASE-T environments. • Autonegotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches. • Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier network administration and troubleshooting. • DTP enables dynamic trunk configuration across all ports in a switch. • PAgP automates the creation of Cisco Fast EtherChannel or Gigabit EtherChannel groups, enabling linking to another switch, router, or server. • Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This is similar to Cisco EtherChannel and PAgP. • IEEE 802.3z-compliant 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, and 1000BASE-T physical interface support through a field-replaceable GBIC module provides customers unprecedented flexibility in switch deployment. • The default configuration stored in Flash memory ensures that the switch can be quickly connected to the network and can pass traffic with minimal user intervention. • The switches support nonstandard Ethernet frame sizes (mini-giants) up to 1542 bytes (configurations with GBIC ports only).

Product Specifications

Feature	Description
Performance	• 13.6-Gbps switching fabric • Cisco Catalyst 2950G-48: 13.6 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950G-24: 8.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950G-24-DC: 8.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950G-12: 6.4 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950T-24: 8.8 Gbps maximum forwarding bandwidth • Cisco Catalyst 2950C-24: 5.2 Gbps maximum forwarding bandwidth (Forwarding rates based on 64-byte packets) • Cisco Catalyst 2950G-48: 10.1-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-24: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-24-DC: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-12: 4.8-Mpps wire-speed forwarding rate • Cisco Catalyst 2950T-24: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950C-24: 3.9-Mpps wire-speed forwarding rate • 8 MB memory architecture shared by all ports • Up to 16 MB SDRAM and 8 MB Flash memory • Configurable up to 8000 MAC addresses • Configurable maximum transmission unit (MTU) of up to 1530 bytes (Cisco Catalyst 2950G switches only)
Management	• [CISCO?] BRIDGE-MIB • CISCO-BULK-FILE-MIB • CISCO-2900-MIB • CISCO-CDP-MIB • CISCO-CLASS-BASED-QOS-MIB • CISCO-CLUSTER-MIB • CISCO-CONFIG-COPY-MIB • CISCO-CONFIG-MAN-MIB • CISCO-ENVMON-MIB • CISCO-FLASH-MIB • CISCO-FTP-CLIENT-MIB • CISCO-IMAGE-MIB • CISCO-IPMROUTE-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-MEMORY-POOL-MIB • CISCO-PAGP-MIB • CISCO-PING-MIB • CISCO-PROCESS-MIB • CISCO-PRODUCTS-MIB • CISCO-RTTMON-MIB • CISCO-SMI • CISCO-STACKMAKER-MIB • CISCO-STP-EXTENSIONS-MIB • CISCO-SYSLOG-MIB • CISCO-TC • CISCO-TCP-MIB

Feature	Description
Management	• CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • ENTITY-MIB • IANAifType-MIB • IF-MIB (RFC 1573) • OLD-CISCO-CHASSIS-MIB • OLD-CISCO-CPU-MIB • OLD-CISCO-INTERFACES-MIB • OLD-CISCO-IP-MIB • OLD-CISCO-MEMORY-MIB • OLD-CISCO-SYSTEM-MIB • OLD-CISCO-TCP-MIB • OLD-CISCO-TS-MIB • RFC1213-MIB (MIB-II) • RFC1398-MIB (ETHERNET-MIB) • RMON-MIB (RFC 1757) • RS-232-MIB • SNMPv2-MIB • SNMPv2-SMI • SNMPv2-TC • TCP-MIB • UDP-MIB
Standards	• IEEE 802.1x support • IEEE 802.1w • IEEE 802.1s • IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning-Tree Protocol • IEEE 802.1p CoS prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10BASE-T specification • IEEE 802.3u 100BASE-TX specification • IEEE 802.3ab 1000BASE-T specification • IEEE 802.3ad • IEEE 802.3z 1000BASE-X specification • 1000BASE-X (GBIC) • 1000BASE-T (GBIC) • 1000BASE-SX • 1000BASE-LX/LH • 1000BASE-ZX • 1000BASE-CWDM GBIC 1470 nm • 1000BASE-CWDM GBIC 1490 nm • 1000BASE-CWDM GBIC 1510 nm • 1000BASE-CWDM GBIC 1530 nm • 1000BASE-CWDM GBIC 1550 nm • 1000BASE-CWDM GBIC 1570 nm • 1000BASE-CWDM GBIC 1590 nm • 1000BASE-CWDM GBIC 1610 nm

Feature	Description
Standards	• RMON I and II standards • SNMPv1, v2c, and v3 (planned future support for v3)
Y2K	• Y2K compliant
Connectors and cabling	• 10BASE-T ports: RJ-45 connectors; two-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling • 100BASE-TX ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 1000BASE-T ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 100BASE-FX ports: MT-RJ connectors, 50/125 or 62.5/125 micron multimode fiber-optic cabling • 1000BASE-T, 1000BASE-SX, -LX/LH, -ZX GBIC-based ports: SC fiber connectors, single-mode or multimode fiber • Cisco GigaStack GBIC ports: copper-based Cisco GigaStack cabling • Management console port: 8-pin RJ-45 connector, RJ-45-to-RJ-45 rollover cable with RJ-45-to-DB9 adapter for PC connections; for terminal connections, use RJ-45-to-DB25 female data-terminal-equipment (DTE) adapter (can be ordered separately from Cisco, part number ACS-DSBUASYN=)
MT-RJ patch cables for Cisco Catalyst 2950C-24 Switch	*Type of cable, Cisco part number* • 1-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-1M • 3-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-3M • 5-meter, MT-RJ-to-SC multimode cable, CAB-MTRJ-SC-MM-5M • 1-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-1M • 3-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-3M • 5-meter, MT-RJ-to-ST multimode cable, CAB-MTRJ-ST-MM-5M
Power connectors	Customers can provide power to a switch by using either the internal power supply or the Cisco RPS 300. The connectors are located at the back of the switch. Internal power supply connector • The internal power supply is an autoranging unit. • The internal power supply supports input voltages between 100 and 240 VAC. • The supplied AC power cord should be used to connect the AC power connector to an AC power outlet. Cisco RPS 675 Connector • The connector offers connection for an optional Cisco RPS 675 that uses AC input and supplies DC output to the switch. • The connector offers a 675-watt redundant power system that can support six external network devices and provides power to one failed device at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • Attach only the Cisco RPS 675 (model PWR675-AC-RPS-NI=) to the RPS receptacle with this connector. Cisco RPS 300 Connector • The connector offers connection for an optional Cisco RPS 300 that uses AC input and supplies DC output to the switch. • The connector offers a 300-watt redundant power system that can support six external network devices and provides power to one failed device at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the RPS receptacle with this connector.

Feature	Description
Indicators	• Per-port status LEDs: link integrity, disabled, activity, speed, and full-duplex indications. • System status LEDs: system, RPS, and bandwidth utilization indications.
Dimensions (H x W x D) and weight	• 1.72 x 17.5 x 9.52 in. (4.36 x 44.5 x 24.18 cm) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, and 2950G-24) • 1.72 x 17.5 x 13 in. (4.36 x 44.5 x 33.02 cm) (Cisco Catalyst 2950G-48) • 1.0 rack-unit (RU) high • 6.5 lb (3.0 kg) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, and 2950G-24) • 10 lb (4.5 kg) (Cisco Catalyst 2950G-48)
Environmental ranges	• Operating temperature: 32 to 113 F (0 to 45 C) • Storage temperature: –13 to 158 F (–25 to 70 C) • Operating relative humidity: 10 to 85 percent (noncondensing) • Operating altitude: Up to 10,000 ft (3000 m) • Storage altitude: Up to 15,000 ft (4500 m) • Not intended for use on top of desktops or in open office environments
Power requirements	• Power consumption: 30W maximum, 102 BTUs per hour (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, and 2950G-24) • Power consumption: 45W maximum, 154 BTUs per hour (Cisco Catalyst 2950G-48) • AC input voltage/frequency: 100 to 127/200 to 240 VAC (autoranging); 50 to 60 Hz • DC input voltages for Cisco RPS 300: +12V @ 4.5A
Acoustic noise	• ISO 7770, bystander position—operating to an ambient temperature of 30 C: – WS-C2950-24, WS-C2950-12, WS-C2950C-24, WS-C2950T-24: 46 dBa – WS-C2950G-12, WS-C2950G-24: 46 dBa – WS-C2950G-48: 48 dBa
Predicted mean time between failure (MTBF)	• 482,776 hours (Cisco Catalyst 2950G-12) • 468,884 hours (Cisco Catalyst 2950G-24) • 479,086 hours (Cisco Catalyst 2950G-24-DC) • 159,026 hours (Cisco Catalyst 2950G-48) • 297,144 hours (Cisco Catalyst 2950T-24) • 268,292 hours (Cisco Catalyst 2950C-24)
Fiber-port specifications for Cisco Catalyst 2950C-24 Switch	Fiber-port power levels: • Optical transmitter wavelength: 1300 nm • Optical receiver sensibility: –14 dBm2 • Optical transmitter power: –19 to –14 dBm • Transmit: –19 to –14 dBm

Feature	Description
Regulatory Agency Approvals	
Safety certifications	• UL 1950/CSA 22.2 No. 950 • IEC 950-EN 60950 • AS/NZS 3260, TS001 • CE Marking
Electromagnetic emissions certifications	• FCC Part 15 Class A • EN 55022: 1998 Class A (CISPR22 Class A) • EN 55024: 1998 (CISPR24) • VCCI Class A • AS/NZS 3548 Class A • CE Marking • CNS 13438 • BSMI Class A • MIC
Network Equipment Building Standards (NEBS) (For WS-C2950G-24-EI-DC only)	• Bellcore • GR-1089-CORE • GR-63-CORE • SR-3580 Level 3
Warranty	• Limited lifetime warranty

Service and Support

The services and support programs described in Table 2 are available as part of the Cisco Desktop Switching Service and Support solution, and are available directly from Cisco and through resellers.

Table 2 Service and Support Programs

Service and Support	Features	Benefits
Advanced Services		
Total Implementation Solutions (TIS)—available direct from Cisco ***Packaged TIS***—available through resellers	• Project management • Site survey and configuration deployment • Installation, text, and cutover • Training • Major moves, adds, and changes • Design review and product staging	• Supplements existing staff • Ensures that functions meet customer needs • Mitigates risk
Technical Support Services		
Cisco SMARTnet® and Cisco SMARTnet Onsite services—available direct from Cisco ***Packaged Cisco SMARTnet service***—available through resellers	• 24x7 access to software updates • Web access to technical repositories • Telephone support through the Cisco Technical Assistance Center (TAC) • Advance replacement of hardware parts	• Enables proactive or expedited issue resolution • Lowers cost of ownership by using Cisco expertise and knowledge • Minimizes network downtime

Ordering Information

Model Numbers	Configuration
WS-C2950G-48-EI	• 48 10/100 ports and 2 1000BASE-X ports • Cisco EI Software image installed
WS-C2950G-24-EI	• 24 10/100 ports and 2 1000BASE-X ports • Cisco EI Software image installed
WS-C2950G-24-EI-DC	• 24 10/100 ports and 2 1000BASE-X ports; DC power • Cisco EI Software image installed
WS-C2950G-12-EI	• 12 10/100 ports and 2 1000BASE-X ports • Cisco EI Software image installed
WS-C2950T-24	• 24 10/100 ports and 2 1000BASE-T ports • Cisco EI Software image installed
WS-C2950C-24	• 24 10/100 ports and 2 100BASE-FX ports • Cisco EI Software image installed
WS-C2950ST-24-LRE	• 24 LRE ports, 2 fixed 10/100/1000BASE-T ports, and 2 SFP ports • Cisco EI Software image installed
WS-C2950ST-8-LRE	• 8 LRE ports, 2 fixed 10/100/1000BASE-T ports, and 2 SFP ports • Cisco EI Software image installed

For More Information

- United States and Canada: 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- http://www.cisco.com

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice FN

CiscoWorks LAN Management Solution 2.2 Introduction

CiscoWorks LAN Management Solution (LMS) provides a robust set of applications for maintaining, monitoring, and troubleshooting a broad range of devices in an end-to-end Cisco AVVID (Architecture for Voice, Video and Integrated Data) network. Built upon popular Internet-based standards, CiscoWorks LMS enables network operators to more efficiently and effectively manage the network through a simplified browser-based interface that can be accessed anytime from anywhere within the network. Taking advantage of a Web-based client/server architecture, CiscoWorks LMS can be easily integrated with other popular network management systems or other third-party management solutions running in the network.

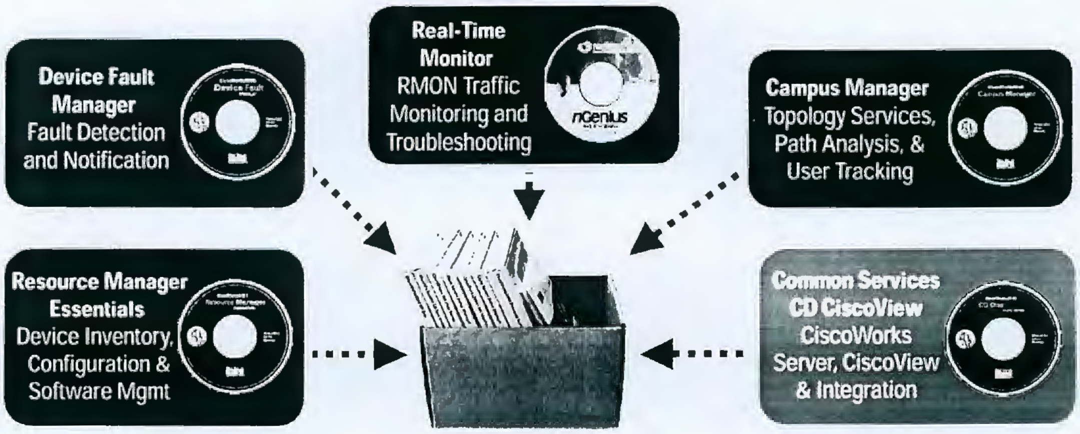
CiscoWorks LMS provides a solid foundation of basic and advanced management applications that complement CiscoWorks products. Other CiscoWorks products include the CiscoWorks Routed WAN Management (RWAN) Solution, which addresses the needs of the WAN with response time and access list management. The IP Telephony Environment Monitor (ITEM) ensures the readiness and manageability of converged networks that support voice over IP (VoIP) and IP telephony traffic and applications. The Cisco VPN/Security Management Solution (VMS) provides an integrated set of Web applications with features that assist in the deployment and monitoring of virtual private network (VPN) and security devices. Together, CiscoWorks products offer leading-edge solutions for improving the accuracy and efficiency of your operations staff, increasing overall availability of your network through proactive planning and maximizing network security.

The Changing Campus LAN

A key part of the business infrastructure, today's LANs are critical systems. The management of local-area networks has evolved from being device centric, to now focusing on managing the convergence of both data and voice traffic over a common infrastructure. As a result, it has become increasingly important to isolate, troubleshoot, and monitor network devices so that connections and services are always available. CiscoWorks LMS delivers advanced discovery technologies, port assignment tools, sophisticated connectivity analysis, configuration management tools, and device and network diagnostic capabilities (including fault management and Remote Monitoring [RMON] traffic monitoring) to help manage the complexities of a converged network.

A Comprehensive Solution

CiscoWorks LMS combines applications and tools for configuring, monitoring, and troubleshooting the campus network. Designed to address the networks powered by Cisco today, it also provides a flexible framework to address the device management needs of networks converging voice, video, and data; networks being protected with Cisco SAFE Blueprint for network security technologies; and networks designed for content migration.


Device Fault Manager
Fault Detection and Notification
Real-Time Monitor
RMON Traffic Monitoring and Troubleshooting
nGenius
Campus Manager
Topology Services, Path Analysis, & User Tracking
Resource Manager Essentials
Device Inventory, Configuration & Software Mgmt
Common Services CD CiscoView
CiscoWorks Server, CiscoView & Integration

The CiscoWorks LMS consists of operationally focused tools. These tools include fault management, scalable topology views, sophisticated configuration, Layer 2/3 path analysis, voice-supported path trace, traffic monitoring, end-station tracking workflow application servers management, and device troubleshooting capabilities.

CiscoWorks LMS is built on the CiscoWorks common services foundation. This design facilitates operations workflow between applications by linking data collection, monitoring, and analysis tools—all from a single desktop application. For example, a user complaint of slow response time or a poor IP phone connection can be quickly diagnosed using CiscoWorks LMS Layer 2 path tools that automatically acquire user path information stored in one database, and highlight devices on a topology map. Additionally, switch or router configurations can then be quickly examined, or RMON traffic data can be reviewed to detect anomalies or the need for changes. Those actions may draw information from one or more applications.

CiscoWorks LMS uses Internet standards to tie together best-of-breed tools and to take advantage of their capabilities through data and task integration standards. Using the common information model (CIM) and Extensible Markup Language (XML), the industry standards for data-sharing CiscoWorks LMS offers a means of extracting data and using it with popular network management platform products. With the CiscoWorks LMS, Cisco offers a complete family of dedicated hardware Cisco Catalyst® network analysis modules (NAMs). Cisco Catalyst NAMs provide increased visibility into switched LAN environments comprising 10/100 and Gigabit Ethernet links for comprehensive, end-to-end, seven-layer monitoring of network infrastructures.

Solution Components

The following applications are included in CiscoWorks LMS:

- CiscoWorks Campus Manager—CiscoWorks Campus Manager is a suite of Web-based applications designed for managing networks powered by Cisco switches. These include Layer 2 device and connectivity discovery, workflow application server discovery and management, detailed topology views, virtual LAN/LAN Emulation (VLAN/LANE) and ATM configuration, end-station tracking, Layer2/3 path analysis tools, and IP phone user and path information.
- CiscoWorks Device Fault Manager—CiscoWorks Device Fault Manager provides real-time fault analysis for Cisco devices. It generates "intelligent Cisco traps" through a variety of data collection and analysis techniques. These can be locally displayed, e-mailed, or forwarded to other popular event management systems.
- nGenius Real-Time Monitor—The nGenius Real-Time Monitor is a Web-enabled multiuser traffic management tool set that provides access to network-wide, real-time RMON information for monitoring, troubleshooting, and maintaining network availability. Its applications graphically report and analyze device, link, and port level RMON collected traffic data from RMON-enabled Cisco Catalyst switches and internal network analysis module.
- CiscoWorks Resource Manager Essentials (RME)—CiscoWorks RME provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis.
- CiscoView—CiscoView is a Web-based tool that graphically provides real-time status of Cisco devices. The tool can drill down to display monitoring information on interfaces and access configuration functions.
- CiscoWorks Management Server—The CiscoWorks Management Server provides the common management desktop services and security across the CiscoWorks Family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications.

Key Functions and Applications

Table 1 gives key functions and applications of the CiscoWorks LMS.

Table 1 CiscoWorks LAN Management Solution Key Application/Function

	Product	Management Benefit
Offers intelligent, automatic discovery of Cisco devices to create topology views of the network	CiscoWorks Campus Manager	The Cisco Campus Manager Topology Services functionality discovers Cisco devices and calculates Layer 2 relationships to provide views of the Cisco network by ATM domain, VTP[1] domain, LAN edge view, and a general Layer 2 view.
Gives topology status indications	CiscoWorks Campus Manager	The topology maps indicate the discovery and SNMP[2] status of Cisco devices; these maps also are launching points for other CiscoWorks applications.
Configures, manages, and monitors VLAN[3] and ATM services/networks	CiscoWorks Campus Manager	CiscoWorks Campus Manager provides tools for creating, deleting, and editing VLANs; it provides ATM tools for displaying virtual circuits and for configuring SPVCs/SPVPs.[4]

Table 1 CiscoWorks LAN Management Solution Key Application/Function

	Product	Management Benefit
Discovers end stations and IP phones connected to switch ports and identifies user locations based on user ID	CiscoWorks Campus Manager	The CiscoWorks Campus Manager User Tracking functionality correlates MAC[5] address and IP address to switch port; integration with Microsoft's PDC and Novell's NDS tree provides the user ID for even more efficient user location and tracking.
Traces Layer 2 and Layer 3 connectivity between two points (devices, servers, phones) in the network	CiscoWorks Campus Manager	The CiscoWorks Campus Manager Path Analysis tool performs path analysis for Layer 2 and Layer 3 devices using the device host name or IP address, and shows results on a map display, in a table display, or in a trace display.
Intelligently analyzes fault conditions designed to detect problems before they become network disruptions	CiscoWorks Device Fault Manager	CiscoWorks Device Fault Manager automated fault detection recognizes common problems in networks without forcing users to define their own rules sets, SNMP trap filters, or device polling intervals.
Interprets fault conditions at both the device and VLAN levels	CiscoWorks Device Fault Manager	With the characteristics of over a 100 Cisco routers and switches predefined, new device support is easily added via Cisco.com. Cisco Device Fault Manager simplifies managing both Layer 2 and Layer 3 environments.
Collects RMON/RMON2 statistics from LAN switches, NAMs, and legacy Cisco SwitchProbe® devices	nGenius Real-Time Monitor	nGenius Real-Time Monitor monitors LAN traffic for protocols, applications, and interfaces to apply appropriate filters, reducing costs and increasing performance.
Provides for LAN troubleshooting at network and application packet levels	nGenius Real-Time Monitor	nGenius Real-Time Monitor helps resolve network and application issues by providing total network visibility from the application layer down to the data link layer for virtually any topology that exists today.
Offers detailed software and hardware inventory reporting	Cisco RME	Cisco RME provides accurate Cisco inventory baseline information, including memory, slots, software versions, and boot ROMs needed to make decisions about the network.
Offers automated update engines for device software and configuration changes	Cisco RME	Cisco RME allows software and configuration updates to be sent to selected devices on a scheduled basis; it reduces time and errors involved in network updates.
Offers a consolidated troubleshooting tools device center	Cisco RME	A wide collection of switch and router analysis tools is accessible from a single location; third-party applications can link to the device center.
Offers centralized change audit logging	Cisco RME	A comprehensive change-monitoring log records users and applications that are active on the network.
Offers graphical device management	CiscoView	CiscoView displays a browser representation of Cisco router and switch devices, color-coded to indicate operational states, with access to configuration and monitoring tools.

Table 1 CiscoWorks LAN Management Solution Key Application/Function

	Product	Management Benefit
Provides application access security	CiscoWorks Server	The CiscoWorks desktop controls user access to applications, ensuring that only appropriate classes of users can access tools that change network parameters versus read-only tools.
Offers third-party integration tools (Integration utility)	CiscoWorks Management Server	The CiscoWorks Management Server simplifies the Web integration of third-party and other Cisco management tools.

1. Virtual Trunking Protocol
2. Simple Network Management Protocol
3. Virtual LAN
4. Soft permanent virtual circuits/soft permanent virtual paths
5. Media Access Control

Key Functions and Applications

Deployment Options

Consider the following when installing the CiscoWorks LAN Management Solution:

- All applications do not have to be installed initially; applications not installed initially may be installed later.
- Most applications require the CiscoWorks Management Server from the Common Services CD (formerly CD One), which must be installed first.
- The CiscoWorks Campus Manager application depends on CiscoWorks RME, which is included as part of the CiscoWorks LAN Management Solution.

All solutions can coexist on the same server if they support and operate with the services of Common Services 2.2. However, network managers may want to consider such factors as the number of applications hosted, system resources, and number of devices to be managed in determining if all or a subset of the solutions are installed on the same server.

CiscoWorks solutions offer deployment flexibility. System administrators should use the guidelines given previously when planning the deployment of the various solution bundles. Some components within a solution require the CiscoWorks Management Server and must be installed on that machine. CiscoView and nGenius Real Time Monitor software can be set up on an independent server. The placement of components is a function of performance requirements and the size of the network.

Server System Requirements

Hardware/Operating System

UNIX

- System: Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) running Solaris 2.8 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM for workstations, 2-GB RAM for servers, 8-MB e-cache

- Available disk: 40-GB internal FC-AL disk drive for workstation and dual drives of this type for server configurations

Windows

- System: IBM PC compatible with 550-MHz or higher Pentium III processor running Microsoft Windows 2000 Advanced Server (with Terminal Services turned off), Server or Professional Edition with Service Pack 2 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM
- Available disk: 40 GB with 2-GB swap recommended

Note: These system requirements are based on managing 500 devices with CiscoWorks RWAN and LAN Management solutions loaded on a single server. Refer to the Installation documentation for more information on required operating system patches.

Client Browser System Requirements

Hardware/Operating System

UNIX

- System: Sun Ultra 10 running Solaris Version 2.7 or 2.8
- System: HP9000 Series running HP-UX 11.0
- System: IBM RS/6000 workstation running AIX 4.3.3
- Memory: 256 MB

Windows

- System: IBM PC-compatible computer with 300-MHz or higher Pentium processor running Windows XP Professional, Windows 2000 (Advanced Server, Server or Professional) with Service Pack 3
- Memory: 256 MB

Note: Refer to the installation documentation for more information on required operating system patches.

Web Browser

UNIX

- Solaris: Netscape v4.76
- HP-UX: Netscape v4.78, 4.79
- AIX: Netscape v4.78, 4.79

Windows

- Windows 2000/XP: Netscape v4.78, 4.79
- Windows 2000/XP: Internet Explorer v6.0.26

Note: Refer to the Installation documentation for more information on required operating systems patches, browser plug-ins, or Java Virtual Machine (JVM) versions.

Service and Support

CiscoWorks products are covered by the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 7 x 24 access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A Cisco SAS contract ensures that customers have easy access to the information and services needed to stay up-to-date with newly supported device packages, patches, and minor updates. For further information on service and support offerings, contact your local sales office.

Ordering Information

The CiscoWorks LAN Management Solution includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris Workstation/Server. The products within this solution can be combined with other CiscoWorks products if they support the same CiscoWorks Management Server version, operating environment, and system requirements. Contact your local Cisco representative for available white papers and documentation outlining best practices for implementing a CiscoWorks management solution architecture.

To place an order, contact your Cisco sales representative.

Refer to the CiscoWorks LAN Management Solution individual product data sheets for more information on operating environment and system requirements.

For More Information

For more information on the CiscoWorks LAN Management Solution, visit http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2425/index.html.

Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

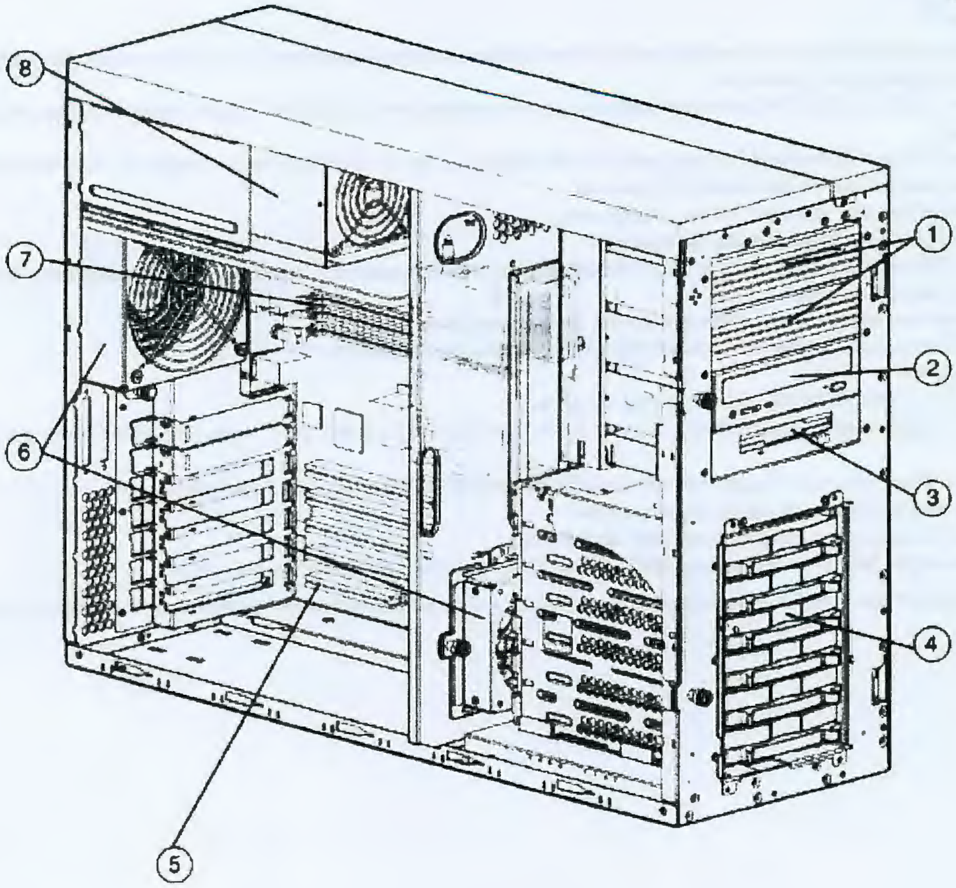
Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice FO

Overview



1. Two Removable Media Bays
2. 48X Max IDE (ATAPI) CD-ROM Drive
3. 1.44 Floppy Drive
4. Six 1" Hot Plug Drive Bays
5. Five expansion slots(four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI)
6. System fan
7. DIMM sockets for up to 8GB of memory, optionally interleaved
8. Optional 2nd Power Supply for hot-pluggable 1+1 redundancy

What's New

- Now available with Intel®Xeon 2.8 GHz Processors with 533MHz system bus.

Overview

At A Glance

- The ProLiant ML350 G3 is an expandable rack or tower platform delivering affordable 2-way performance and essential availability to corporate workgroups and growing businesses
- Intel Xeon 2.4 GHz or 2.8 GHz processors (dual processor capability) with 512-KB level 2 cache standard (full speed) and Hyper-Threading Technology
- ServerWorks Grand Champion LE Chipset with 533-MHz Front Side Bus for 2.8GHz processor models or 400-MHz FSB for models < 2.8 GHz
- Integrated Dual Channel Wide Ultra3 SCSI Adapter
- Smart Array Controller (standard in Array Models only)
- NC7760 PCI Gigabit Server Adapter (embedded)
- 512MB of 2-way interleaving capable PC2100 DDR SDRAM, with Advanced ECC capabilities (Array models only; 256MB standard on other models): Expandable to 8GB
- Flexible memory configurations allow interleaving (2x1) or non-interleaving
- Five available expansion slots: four 64-bit/100-MHz PCI-X, one 32-bit/33-MHz PCI
- Two USB ports
- Standard 6 x 1" Wide Ultra320 ready Hot Plug Drive Cage
- Internal storage capacity of up to 880GB (6 x 146.8 GB 1"), 1.174-TB (2 x 146.8 GB 1" + 6 x 146.8 GB 1") with optional 2-bay hot plug drive cage option
- 500W Hot-Pluggable Power Supply (standard) and an optional 500W Hot-Pluggable Redundant Power Supply (1+ 1) available
- Tool-free entry to chassis and access to components
- RBSU (ROM based setup utility) support, redundant ROM
- Insight Manager, SmartStart, ROM-based BIOS Setup Utility, and Automatic Server Recovery (ASR-2)
- Protected by HP Services, including a three-year, next business day, on-site, limited global warranty and extended Pre-Failure Warranty.

Standard Features

Processor *One of the following depending on Model:*	Intel Xeon Processor 2.8 GHz/533-512KB Intel Xeon Processor 2.4 GHz/400-512KB
Cache Memory	Integrated 512-KB Level 2 cache (full speed)
Upgradability	Upgradable to dual processing
Chipset	ServerWorks Grand Champion LE Chipset with 400-MHz or 533-MHz Front Side Bus (model dependent) NOTE: For more information regarding ServerWorks, please see the following URL: http://www.serverworks.com/products/overview.html NOTE: This Web site is available in English only.
Memory (One of the following depending on model)	2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advonced ECC capabilities Standard (Non-Array Models) 256MB Standard (Array Models) 512MB Moximum 8 GB
Network Controller	NC7760 Gigabit Server Adapter (embedded)

Expansion Slots

I/O (5 Total, 5 Available)		PCI Voltage:
64-bit/100MHz, PCI	4 (4 available) (Array model has 3 available)	3.3 Volt or universal cards
32-bit/33MHz, PCI	1 (1 available)	5 Volt or universal cards

Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 641 Controller (2.8 GHz Array Models Only)

Storage

Diskette Drives	1.44 MB
CD-ROM	48x IDE (ATAPI) CD-ROM Drive
Hard Drives	None
Maximum Internal Storage	1.174 TB GB (6 x 146.8 GB 1" with standard internal hot plug drive cage + (2 x 146.8 GB 1") with optional ML3xx Two Bay Hot Plug SCSI Drive Cage)
External Storage	Two external SCSI knockouts available, optional ProLiant ML350 Internal to External SCSI Cable Option Kit required ● HD68 Internal to External SCSI Cable Option Kit PN 159547-B22 ● VHDCI Internal to External SCSI Cable Option Kit PN 333370-B21

Standard Features

Interfaces	Parallel	1
	Serial	1
	Pointing Device (Mouse)	1
	Graphics	1
	Keyboard	1
	Network RJ-45	1
	USB	2 NOTE: Please see the following URL for additional information regarding USB support: http://www.compaq.com/products/servers/platforms/usb-support.html. NOTE: This Web site is available in English only.
	External SCSI knockouts	2

Graphics — Integrated ATI RAGE XL Video Controller with 8-MB SDRAM Video Memory

Form Factor — Tower or rack (5U)

NOTE: Rack models (and rack conversion kit) support:

- Square hole racks from 27"- 32" deep (including Compaq/HP 7000, 9000, 10000 and H9 series)
- Square or round hole racks, from 24" - 35" deep (including HP Rack System /E and HP Systems, with an adjustment)
- Telco racks with 3rd part option kit from Rack Solutions

http://www.racksolutions.com/compaq/products.htm
NOTE: This Web site is available in English only.

ProLiant Essentials Foundation Pack Software

Insight Manager 7

Insight Manager 7 helps maximize system uptime and performance and reduces the cost of maintaining the IT infrastructure by providing proactive notification of problems before those problems result in costly downtime and reduced productivity. Insight Manager 7 is easy to set up and provides rapid access to detailed fault and performance information gathered by the Management Agents. One-click-access to the Remote Insight Lights Out Edition II board allows systems administrators to take full graphical control of ProLiant servers in remote locations or lights-out data centers. Finally, Insight Manager 7 in concert with the Version Control Agents and Version Control Repository Manager enables systems administrators to version manage and update system software across groups of ProLiant servers.

Management Agents

The Management Agents form the foundation for HP's Intelligent Manageability strategy. They provide direct, browser-based access to in-depth instrumentation built into HP servers, workstations, desktops, and portables, and send alerts to Insight Manager 7 and other enterprise management applications in case of subsystem or environmental failures. For additional information about the Management Agents and other management products from HP, please visit the management Web site at http://www.hp.com/servers/manage.

SmartStart

SmartStart is a tool that simplifies server setup, providing a rapid way to deploy reliable and consistent server configurations. For more information, please visit the SmartStart website at http://www.hp.com/servers/manage.
SmartStart version supported (minimum): SmartStart 5.50

ActiveUpdate

ActiveUpdate is a web-based application that keeps IT managers directly connected to HP for proactive notification and delivery of the latest software updates.

ROMPaq, support software, and configuration utilities

The latest software, drivers, and firmware fully optimized and tested for your ProLiant server and options.

Survey Utility and diagnostics utilities

The most advanced configuration analysis, reporting and troubleshooting utilities used by HP and at your fingertips.

Optional Proliant Essentials Value Packs

Optional software offerings that selectively extend the functionality of an Adaptive Infrastructure to address specific business problems and needs:

- Rapid Deployment Pack – an automated solution for multi-server deployment and provisioning, enabling companies to quickly and easily adapt to changing business demands.
- Workload Management Pack – provides easier management of complex environments, improving overall server utilization and enabling Windows 2000 customers for the first time to confidently deploy multiple applications on a single multiprocessor ProLiant Server.
- Performance Management Pack – a performance management solution that identifies and explains hardware performance bottlenecks on ProLiant servers and attached options enabling users to better utilize their valuable resources.

NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Value Packs. Refer to http://www.hp.com/servers/proliantessentials or the various ProLiant Essentials Value Pack product QuickSpecs for more information.
NOTE: For more information regarding ProLiant Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentials
NOTE: These Web sites are available in English only.

Industry Standard Compliance

ACPI V1.0B Compliant
PCI 2.2 Compliant
PXE Support
WOL Support
PCI-X 1.0 Compliant
Novell Certified
Microsoft Logo certifications

Standard Features

Manageability

Insight Manager 7
Redundant ROM
System Firmware Update
ROMPaq
Remote Insight Lights-Out Edition II (optional)
ProLiant RBSU (ROM-Based Setup Utility)
Automatic Server Recovery-2 (ASR-2)
Drive Parameter Tracking (with Smart Array Controller)
Dynamic Sector Repairing (with Smart Array Controller)
Pre-Failure Warranty (covers processors, memory and hard drives)

Security

Power-on password
Setup password
Diskette boot control
Parallel and serial interface control
Disk configuration lock
Power switch security

Server Power Cords

One Lowline NEMA power cord and one Highline IEC Power cord ship standard
Tower models ship with standard country specific power cords.
Rack models ship with IEC cables. Depending on the country, some also ship with country specific power cords
Redundant power supply options ship with country specific power cords with the exception of the -B21 Rack SKU which ships with an IEC cable only.

Power Supply

500 Watts, Power Factor Correction (PFC), Hot Plug 100 to 240 VAC Rated Input Voltage (Auto-sensing), CE Mark Compliant
Optional 2nd Power Supply for hot-pluggable 1 + 1 redundancy.

System Fans

2 fans ship standard, 2 fans total supported (does not include power supply fans)

Required Cabling

For required cabling information, refer to the HP Web site at http://www.hp.com/servers/proliantML350.
NOTE: This Web site is available in English only

OS Support

Microsoft Windows NT® Server 4.0 and Terminal Server 4.0
Microsoft BackOffice Small Business Server 2000
Microsoft Windows 2000 Server and Advanced Server
Windows Server 2003
Novell NetWare 5.1, 6.0
Novell NetWare Small Business Suite 6.0
SCO OpenServer 5.0.6a
SCO OpenUnix 8 SCO UnixWare 7.1.1
IBM OS/2 Warp Server for e-business
LINUX (Red Hat, 2.1 Advanced Server, Red Hat 8.0 and Red Hat 7.3, SuSE, SLES7, UnitedLinux 1.0)
NOTE: For a more complete and up-to-date listing of supported OSs and versions, please visit our OS Support Matrix at: ftp://ftp.compaq.com/pub/products/servers/os-support-matrix-310.pdf
NOTE: Optional hardware may be required to support some operating systems.
NOTE: For an up-to-date listing of the latest drivers available for the ProLiant ML350, please see: http://www.compaq.com/support/files/server/us/index.html.
NOTE: These Web sites are available in English only.

Standard Features

Rack Airflow Requirements

- Rack 9000 and 10000 series Cabinets
  The increasing power of new high-performance processor technology requires increased cooling efficiency for rack-mounted servers. The 9000 and 10000 Series Racks provide enhanced airflow for maximum cooling, allowing these racks to be fully loaded with servers using the latest processors.

- Rack 7000 series Cabinets
  When installing a server with processors running at speeds of 550 MHz or greater in Rack 7000 series racks with glass doors (165753-001 (42U), and 163747-001 (22U)), the new processor technology requires the installation of HP's new High Airflow Rack Door Inserts (327281-B21 (42U), 327281-B22 (42U 6 pack), or 157847-B21 (22U)) to promote enhanced airflow for maximum cooling.

CAUTION: If a third-party rack is used, observe the following additional requirements to ensure adequate airflow and to prevent damage to the equipment:

- Front and rear doors: If your 42U server rack includes closing front and rear doors, you must allow 830 square inches (5,350 sq cm) of hole evenly distributed from top to bottom to permit adequate airflow (equivalent to the required 64 percent open area for ventilation).
- Side: The clearance between the installed rack component and the side panels of the rack must be a minimum of 2.75 inches (7 cm).

CAUTION: Always use blanking panels to fill all remaining empty front panel U-spaces in the rack. This arrangement ensures proper airflow. Using a rack without blanking panels results in improper cooling that can lead to thermal damage.

NOTE: For additional information, refer to the Setup and Installation Guide or the Documentation CD provided with the server, or to the server documentation located in the Support section at the following URL:
http://www5.hp.com/servers/proliantml350
NOTE: This Web site is available in English only.

Installation of Server into Telco Racks

ML350 G3 rack model support: Support for all 2-post Telco racks requires the use of the rack kit and an additional option kit from Rack Solutions. http://www.racksolutions.com/compaq
NOTE: This Web site is available in English only.

HP Factory Express Capabilities

HP Factory Express gives you the flexibility to choose from a full menu of factory capabilities all in one manufacturing facility, in one process, with one touch giving you full control and access to HP's World class manufacturing facility anytime. This approach provides you the speed to deploy your IT needs, with total quality assurance, reliability, and predictability to lower your total cost of ownership by letting HP install, rack, and customize your software and hardware options for you.

Standard Features

Service and Support

HP Services provides a three-year, limited warranty, including Pre-Failure Warranty (coverage of hard drives, memory and processors) fully supported by a worldwide network of resellers and service providers and lifetime toll-free 7 x 24 hardware technical phone support. In addition, available service offerings include:
NOTE: Limited Warranty includes 3 year Parts, 3 year Labor, 3-year on-site support.

A full range of HP Care Pack packaged hardware and software services:

- Installation and start up
- Extended coverage hours and enhanced response times
- System management and performance services
- Availability and recovery services

NOTE: For more infomation, visit http://www.hp.com/services/carepack.

Please see the following URL regarding Warranty Information For Your HP Products:
http://www.compaq.com/support/warranty_upgrades/web_statements/176738.html.

For additional information regarding Worldwide Limited Warranty and Technical Support, please see the following URL:
ftp://ftp.compaq.com/pub/supportinformation/ejourney/176738.pdf.
NOTE: These Web sites are available in English only.

NOTE: Certain restrictions and exclusions apply. Consult the Customer Support Center at 1-800-345-1518 for details

Models

ML350T03 X2.8-512KB/533, 256MB *311523-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)
ML350R03 X2.8-512KB/533, 256MB *311524-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)
ML350T03 X2.8-512KB/533, 512MB Array *311525-001*	Processor(s)	(1) Intel Xeon Processor 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional drive cage & hard drives)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)
ML350R03 X2.8-512KB/533, 512MB Array *311526-001*	Processor(s)	(1) Xeon 2.8 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	512 MB of Advanced ECC PC2100 DDR SDRAM DIMM (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	RAID Controller	Smart Array 641
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

Models

ML350T03 X2.4-512KB/400, 256MB 269786-001	Processor(s)	(1) Intel Xeon Processor 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hard drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Tower (5U)
ML350R03 X2.4-512KB/400, 256MB 269787-001	Processor(s)	(1) Xeon 2.4 GHz Processor standard (up to 2 supported)
	Cache Memory	Integrated 512-KB Level 2 cache per processor
	Memory	256 MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (Standard) to 8 GB (Maximum)
	Network Controller	NC7760 PCI Gigabit Server Adapter (Integrated/Embedded)
	Storage Controller	Integrated Dual Channel Wide Ultra3 SCSI Adapter
	Hard Drive	None ship standard
	Internal Storage	1.174 TB maximum hot plug (with optional hord drives & drive cage)
	Optical Drive	48x IDE (ATAPI) CD-ROM Drive
	Form Factor	Rack (5U)

ProLiant ML350 G3 Unique Options	Hot Plug Redundant Power Supply Option Kit	283655-001
	Hot Plug Redundant Power Supply Option Kit (cable) NOTE: PN 283655-B21 SKU contains the 2nd power supply with an IEC power cable. Only purchase if connecting to PDU/UPS that supports IEC cables. All other SKUs contain country specific power cables.	283655-B21
	Intel Xeon 2.80 GHz-512KB Processor Option Kit NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiant ML350 G3 systems with 533 MHz front side bus only. This kit cannot be used in 400 MHz front side bus systems such as those with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	314763-B21
	Intel Xeon 2.40 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 257913-B21) supports the ProLiant ML350 G3 servers.	257913-B21
	Intel Xeon 2.20 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 283702-B21) supports the ProLiant ML350 G3 servers.	283702-B21
	Intel Xeon 2.0 GHz-512KB Processor Option Kit NOTE: This processor option kit (PN 283701-B21) supports the ProLiant ML350 G3 servers.	283701-B21
	ProLiant ML350 G3 Tower to Rack Conversion Kit (CPQ brand)	290683-B21
ProLiant Essentials Value Pack Software	Rapid Deployment Pack, 1 User, V1.x NOTE: This license allows 1 server to be managed and deployed via the Deployment Server.	267196-B21
	Rapid Deployment Pack, 10 Users, V1.x NOTE: This license allows 10 servers to be managed and deployed via the Deployment Server.	269817-B21
	Flexible Quantity License Kit	302127-B21
	License-Only - for use with a Master License Agreement	302128-B21
	ProLiant Essentials Workload Management Pack 2.0 (Featuring Compaq Resource Partitioning Manager version 2.0)	303284-B21
	ProLiant Essentials Performance Management Pack Flexible License	306697-B21
	NOTE: Flexible and volume quantity license kits are available for ProLiant Essentials Value Packs. Refer to http://www.hp.com/servers/proliantessentials or the various ProLiant Essentials Value Pack product QuickSpecs for more information. NOTE: For more information regarding ProLiant Essentials Software, please see the following URL: http://www.hp.com/servers/proliantessentials. NOTE: These Web sites are available in English only.	
HP NetServer Transition Services	HP NetServer to ProLiant integration and assessment service NOTE: HP identifies current levels of NetServer support, services, and management. This service helps maximize customer's ability to add ProLiant platforms into their current environment.	304164-002
	HP TopTools to Insight Manager 7 installation and startup service NOTE: Provides on-site review, installation and configuration services for Insight Manager 7. HP will also re-create, as closely as possible, the views and reports from the customer's current TopTools configuration. This service assures a smooth transition to the ProLiant Essentials software.	304163-002
	HP NetServer to ProLiant Essentials Rapid Deployment Pack installation and startup service NOTE: Install and configure Rapid Deployment Pack in a test environment, then deploy a server image to a maximum of 250 systems in the production environment. This service helps to assure successful system deployment.	304162-002

Options

Processors

Intel Xeon 2.80 GHz-512KB Processor Option Kit NOTE: The 2.8 GHz processor option kit (PN 314763-B21) supports ProLiant ML350 G3 systems with 533 MHz front side bus only. This kit cannot be used in 400 MHz front side bus systems such os thhose with 2.4 GHz, 2.2GHz or 2.0 GHz processors.	314763-B21
Intel Xeon 2.40 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 257913-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	257913-B21
Intel Xeon 2.20 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283702-B21) cannot be used in 533 MHz front side bus systems such as the 2.8 GHz systems.	283702-B21
Intel Xeon 2.0 GHz-512KB Processor Option Kit NOTE: This processor option kit supports ProLiant ML350 G3 servers with 400 MHz front side bus only. This kit (PN 283701-B21) cannot be used in 533 MHz front side bus systems such os the 2.8 GHz systems.	283701-B21

Memory (DIMMs)

NOTE: The ML350 G3 supports both interleaved and non-interleaved memory configurotions. Bose models ship standord with one 256MB DIMM or one 512MB DIMM (Array models). For best performance automatically invoke interleaving by populating memory in identical pairs. If 1GB of total memory is desired odd three 256MB DIMMs to the base configuration. If 1.5GB of memory is desired add one 256MB DIMM (to pair with the standard DIMM) and two 512MB DIMMs. Interleaving and installation of memory in pairs is not required. Add any combination of memory DIMMs below to operate in non-interleaved mode.
NOTE: Each SDRAM Memory kit contains one (1) DIMM.

128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21
512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21
1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21

Internal Storage

ML3xx Two Bay Hot Plug SCSI Drive Cage NOTE: The drive cage option kit (PN 244059-B21) has one 1' drive bay and one 1.6" drive bay. It installs in two available removoble media boys	244059-B21

Optical Drives

16X DVD-ROM Drive Option Kit (Carbon)	217053-B21
CD-RW/DVD-ROM 48X Combo Drive Option Kit	33134

Hard Drives

Ultra320 – Universal Hot Plug

146.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286716-B22
72.8-GB 10,000 rpm U320 Universal Hard Drive (1")	286714-B22
36.4-GB 10,000 rpm U320 Universal Hard Drive (1")	286713-B22
72.8-GB 15,000 rpm U320 Universal Hard Drive (1")	286778-B22
36.4-GB 15,000 rpm U320 Universal Hard Drive (1")	286776-B22
18.2-GB 15,000 rpm U320 Universal Hard Drive (1")	286775-B22

NOTE: All U320 Universal Hard Drives are backward compotible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates.

NOTE: Please see the Wide Ultra320 Universal Hot Plug QuickSpecs for additional technical information on the hard drives Support details, please see the following:
http://www5.compaq com/products/quickspecs/11531_na/11531_na.HTML

Storage Controllers	Smart Array 6402/128 Controller	273915-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Compaq RAID LC2 Controller	188044-B21
	Smart Array 532 Controller	225338-B21
	Smart Array 5302/128 Controller	283552-B21
	Smart Array 5304/256 Controller	283551-B21
	Smart Array 5312 Controller	238633-B21
	Smart Array 641 Controller	291966-B21
	Smart Array 642 Controller	291967-B21
	Ultra3 Channel Expansion Module for Smart Array 5300 Controller	153507-B21
	128-MB Cache Module for Smart Array 5302 Controller	153506-B21
	RAID ADG Upgrade for Smart Array 5302	288601-B21
	256-MB Battery Backed Cache Module NOTE: This 256-MB Battery Backed Cache Module supports the Smart Array 5300 series controllers, MSA 1000 and the Smart Array Cluster Storage.	254786-B21
	256MB Cache Upgrade for SA-6402 NOTE: This 256-MB Battery-Backed Cache Module upgrade kit supports the Smart Array 6400 series controller only.	273913-B21
	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS	284688-B21
	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter	268351-B21

NOTE: Please see the following Controller or SCSI Adapter QuickSpecs for Technical Specifications such as PCI Bus, PCI Peak Data Transfer Rate, SCSI Protocols supported, SCSI Peak Data Transfer Rate, Channels, SCSI Ports, Drives supported, Cache, RAID support, and additional information:

http://www5.compaq.com/products/quickspecs/10652_na/10652_na.HTML
(RAID LC2)

http://www5.compaq.com/products/quickspecs/10851_na/10851_na.HTML
(Smart Array 532)

http://www5.compaq.com/products/quickspecs/10640_na/10640_na.HTML
(Smart Array 5300 Series)

http://www5.compaq.com/products/quickspecs/11328_na/11328_na.HTML
(Smart Array 5312)

http://www5.compaq.com/products/quickspecs/11587_na/11587_na.HTML
(Smart Array 6402)

http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML
(Smart Array 641)

http://www5.compaq.com/products/quickspecs/11563_na/11563_na.HTML
(Smart Array 642)

http://www5.compaq.com/products/quickspecs/10429_na/10429_na.HTML
(SCSI Adapter)

http://www5.compaq.com/products/quickspecs/11555_nav/11555_na.HTML
(U320 Adapter)

Wireless HAP Solution	Compaq WL410 Wireless SMB Access Point	191811-001

Options

Communications	NC3123 Fast Ethernet NIC PCI 10/100 WOL and PXE	174830-B21
	NC3134 Fast Ethernet NIC 64 PCI Dual Port 10/100	138603-B21
	NC3135 Fast Ethernet Module Dual 10/100 Upgrade Module for NC3134	138604-B21
	NC6132 1000 SX Upgrade Module for NC3134	338456-B23
	NC6136 Gigabit Server Adapter, 64-bit/66MHz, PCI, 1000 SX	203539-B21
	NC6170 Dual Port PCI-X 1000SX Gigabit Server Adapter	313879-B21
	NC6770 PCI-X Gigabit Server Adapter, 1000-SX	244949-B21
	NC7170 Dual Port PCI-X 1000T Gigabit Server Adapter	313881-B21
	NC7132 Gigabit Upgrade Module 10/100/1000-T	153543-B21
	NC7770 PCI-X Gigabit server adapter	244948-B21
	56K v.90 PCI Modem	239137-001
	NOTE: Any NC31XX, NC61XX, NC71XX or NC77XX NIC can be used for redundancy with the embedded NC7760 Network Controller.	
Management Options	Remote Insight Lights-Out Edition II	227251-001
Security	HP/Atalla AXL600L SSL Accelerator Card for ProLiant Servers	524545-B21
Monitors	*Essential Series*	
	Compaq S9500 CRT Monitor (19-inch, Carbon/Silver)	261615-003
	Compaq S7500 CRT Monitor (17-inch, Carbon/Silver)	261606-001
	Compaq S5500 CRT Monitor (15-inch Carbon/Silver)	261602-001
	Compaq TFT1501 Flat Panel Monitor (15-inch, Carbon/Silver)	301042-003
	Compaq TFT1701 Flat Panel Monitor (17-inch, Carbon/Silver)	292847-003
	Advantage Series	
	Compaq V7550 CRT Color Monitor (17-inch, Carbon/Silver)	261611-003
	Compaq TFT1720 Flat Panel Monitor (17-inch, Carbon/Silver)	295926-003
	Compaq FT1720M Flat Panel Monitor (17-inch, Carbon/Silver, includes speaker, USB port, headphone)	301958-003
	Compaq TFT1520 Flat Panel Monitor (15-inch, Carbon/Silver)	295925-003
	Compaq TFT1520M Flat Panel Monitor (15-inch, Carbon/Silver includes speaker, USB port, headphone)	301957-003
	Performance Series	
	HP P930 CRT Monitor (19-inch, Flat-screen, Carbon/Silver)	302268-003
	HP P1130 CRT Monitor (21-inch, Flat-screen, Carbon/Silver)	302270-003
	HP L1825 Flat Panel Monitor (18-inch, Carbon/Silver)	303486-003
	HP L2025 Flat Panel Monitor (20-inch, Carbon/Silver)	303102-003
	Compaq TFT1825 Flat Panel Monitor (18-inch, Carbon/Silver)	296751-003
	Compaq TFT2025 Flat Panel Monitor (20-inch, Carbon/Silver)	285550-003
	Rackmount Flat Panel Monitors	
	TFT5110R Flat Panel Monitor (Carbon)	281683-B21
	NOTE: Monitors larger than 17" may be too heavy for use in rack systems.	

Tape Drives

NOTE: In order to install certain tape drives internally, you may need to remove the rails that come standard on the drives and then re-insert the screws in the mounting holes. To ensure proper fit, install the mounting screws as described in the tape option kit.

Internal and External DAT Tape Drives

Internal 12/24-GB DAT Drive (Opal)	295513-B22

NOTE: Please see the 12/24-GB DAT Drive QuickSpecs for additional options such as cassettes and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/10239_na/10239_na.HTML

HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, Internal (Carbon)	157769-B22
HP StorageWorks 20/40-GB DAT DDS-4 Tape Drive, External (Carbon)	157770-002
HP StorageWorks Internal 20/40-GB DAT, Hot Plug (Carbon)	215488-B21

NOTE: Please see the 20/40-GB DAT Tape Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10426_na/10426_na.HTML

Internal and External DAT 72 Tape Backup Drive

HP StorageWorks DAT 72 Tape Drive Internal (Carbon)	Q1525A
HP StorageWorks DAT 72 Tape Drive, External (Carbon)	Q1527A
HP StorageWorks DAT 72h Internal Hot Plug (Carbon)	Q1529A

NOTE: Please see the DAT 72 Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11597_na/11597_na.HTML

Internal and External LTO Ultrium Tape Drives

HP StorageWorks Ultrium 215 Tape Drive for ProLiant, Internal (Carbon)	Q1543A
HP StorageWorks Ultrium 215 Tape Drive for ProLiant, External (Carbon)	Q1544A

NOTE: Please see the HP StorageWorks Ultrium 230 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://h18006.www1.hp.com/products/quickspecs/11678_na/11678_na.html

HP StorageWorks LTO Ultrium 230 Tape Drive, Internal (Carbon)	Q1515A
HP StorageWorks LTO Ultrium 230 Tape Drive, External (Carbon)	Q1516A

NOTE: Please see the HP StorageWorks LTO Ultrium QuickSpecs for additional options such as data and cleaning cartridges, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11415_na/11415_na.HTML

HP StorageWorks Ultrium 460 tape drive for ProLiant, Internal (Carbon)	Q1518A
HP StorageWorks Ultrium 460 tape drive for ProLiant, External (Carbon)	Q1519A

NOTE: Please see the HP StorageWorks Ultrium 460 Tape Drive QuickSpecs for additional options such as controllers, and other related items, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11530_na/11530_na.HTML

Options

Internal and External AIT Tape Drives

NOTE: The Internal AIT Hot Plug Drives are supported in hot plug drive bays only. When installing a non hot plug AIT tape drive into an ML350 ProLiant server use the special screw included with the drive kit proper fit in the removable media bay.

HP StorageWorks Internal AIT 35-GB, LVD Tape Drive (Carbon)	216884-B21
HP StorageWorks External AIT 35-GB, LVD Tape Drive (Carbon)	216885-001
HP StorageWorks Internal AIT 35-GB, LVD, Hot Plug (Carbon)	216886-B21

NOTE: Please see the AIT 35-GB, LVD Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10712_na/10712_na.HTML

HP StorageWorks AIT 50-GB Tape Drive, Internal (Carbon)	157766-B22
HP StorageWorks AIT 50-GB Tape Drive, External (Carbon)	157767-002
HP StorageWorks Internal AIT 50-GB, Hot Plug (carbon)	215487-B21
HP StorageWorks Rackmount AIT 50-GB, 3U (Single Drive)	274333-B21

NOTE: Please see the AIT 50-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10425_na/10425_na.HTML

HP StorageWorks Internal AIT 100-GB Tape Drive (Carbon)	249189-B21
HP StorageWorks External AIT 100-GB Tape Drive (Carbon)	249160-001
HP StorageWorks Internal AIT 100-GB, Hot-Plug (Carbon)	249161-B21

NOTE: Please see the AIT 100-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11062_na/11062_na.HTML

Internal and External DLT/SDLT Tape Drives

NOTE: When installing a DLT or SDLT tape drive into a ProLiant ML350, use the special screw included with the drive kit to ensure proper fit in the removable media bay.

HP StorageWorks 40/80-GB DLT Tape Drive, Internal (Carbon)	146196-B22
HP StorageWorks 40/80-GB DLT Tape Drive, External (Carbon)	146197-B23
HP StorageWorks Rackmount DLT 40/80, 3U (Single Drive)	274332-B21
HP StorageWorks Rackmount DLT 40/80, Dual-Drive, 3U (Two Drives)	274335-B21
HP StorageWorks Rackmount DLT 40/80, Tape Array III, 5U (Four Drives)	274337-B21

NOTE: Please see the 40/80-GB DLT Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10658_na/10658_na.HTML

HP StorageWorks DLT VS 40/80 Tape Drive, Internal (Carbon)	280129-B21
HP StorageWorks DLT VS 40/80 Tape Drive, External (Carbon)	280129-B22

NOTE: Please see the 40/80-GB DLT VS Drive QuickSpecs for additional options such as host bus adapters, controllers, cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11403_na/11403_na.HTML

HP StorageWorks SDLT 110/220, Internal (carbon)	192106-B25
HP StorageWorks SDLT 110/220, External (Carbon)	192103-002
HP StorageWorks Rackmount SDLT 110/220, 3U (Single Drive)	274331-B21
HP StorageWorks Rackmount SDLT 110/220, Dual-Drive, 3U (Two Drives)	274334-B21
HP StorageWorks Rackmount SDLT 110/220, Tape Array III, 5U (Four Drives)	274336-B21

NOTE: Please see the SDLT 110/220-GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10772_na/10772_na.HTML

HP StorageWorks SDLT 160/320, Internal (carbon)	257319-B21
HP StorageWorks SDLT 160/320, External (carbon)	257319-001

NOTE: Please see the SDLT 160/320GB Tape Drive QuickSpecs for additional options such as adapters, controllers, and media, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/11406_na/11406_na.HTML

Internal and External DAT Autoloader

20/40-GB DAT 8 Cassette Autoloader Internal (Opal)	166504-B21
20/40-GB DAT 8 Cassette Autoloader External (Opal)	166505-001

NOTE: Please see the 20/40-GB DAT DDS-4 8 Cassette Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following:
http://www5.compaq.com/products/quickspecs/10518_na/10518_na.HTML

Options

AIT Autoloader	
HP StorageWorks AIT 35GB Autoloader, Rackmount (carbon)	280349-001
HP StorageWorks AIT 35GB Autoloader Tabletop (carbon)	292355-001
NOTE: Please see the HP StorageWorks AIT 35GB Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/11404_na/11404_na.HTML	
HP StorageWorks 1/8 Autoloader	
HP StorageWorks 1/8 Autoloader, Tabletop, Ultrium 230	C9572CB
HP StorageWorks 1/8 Autoloader, Tabletop, DLT VS80	C9264CB
HP StorageWorks 1/8 Autoloader, Rackmount kit	C9266R
NOTE: Please see the HP StorageWorks 1/8 Autoloader QuickSpecs for additional options such as adapters, controllers, and cassettes, and for an up-to-date listing of the latest O/S Support details, please see the following: http://www5.compaq.com/products/quickspecs/11496_na/11496_na.HTML	
SSL1016 tape autoloader	
SSL1016 DLT1 tape autoloader (includes two 8-cartridge magazines and a barcode reader)	330815-B21
NOTE: Please see the SSL1016 DLT1 tape autoloader Quick Specs for additional information: http://h18000.www1.hp.com/products/quickspecs/11626_na/11626_na.HTML	
SSL1016 SDLT 160/320 tape autoloader (includes two 8-cartridge magazines and a barcode reader)	330816-B21
NOTE: Please see the SSL1016 SDLT160/320 tape autoloader Quick Specs for additional information: http://h18000.www1.hp.com/products/quickspecs/11609_na/11609_na.HTML	
Add-on drives and accessories	
SSL1016 DLT/SDLT 8-cartridge magazine	268664-B22
Rackmount Tape Drive Kits	
3U Rackmount Kit	274338-B21
NOTE: The 3U Rackmount Kit (PN 274338-B21) can support up to (2) full-height or (4) half-height tape drives and compatible with multiple Single-Ended and LVD SCSI Tape Drives including the 12/24-GB DAT, 20/40-GB DAT, DAT 72-GB, 20/40-GB DAT DDS-4 8 Cassette Autoloader, AIT 35GB LVD, AIT 50GB, AIT 100-GB, 40/80-GB DLT, DLT VS 40/80-GB, SDLT 110/220-GB, SDLT 160/320-GB, Ultrium 215, Ultrium 230 and Ultrium 460 Tape Drives.	
5U Rackmount Kit	274339-B21
NOTE: The 5U Rackmount Kit (PN 274339-B21) can support up to (4) full-height tape drives and is compatible with DLT/SDLT/LTO tape drives including the 40/80-GB DLT, SDLT 110/220, SDLT 160/320, Ultrium 230, and Ultrium 460 Tape Drives.	
NOTE: Please see the Rackmount Tape Drive Kits QuickSpecs for additional information regarding these kits, please see the following: http://www5.compaq.com/products/quickspecs/10854_na/10854_na.HTML	
Tape Storage Enclosure Cable Kits	
LVD Cable Kit, VHDCI/HD68	168048-B21
NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Array III only.	
LVD Cable Kit, HD68/HD68	242381-B21
NOTE: For use with the 3U RM Storage Enclosure and DLT Tape Array III only	

Tape Automation

StorageWorks SSL2000 small system library

SSL2020 – AIT50 based library with up to 2 drives and 20 slots

SSL2020 AIT Mini-Library 1 drive, 20 slot Table Top	175195-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Table Top	175195-B22
SSL2020 AIT Mini-Library 1 drive, 20 slot Rackmount	175196-B21
SSL2020 AIT Mini-Library 2 drive, 20 slot Rackmount	175196-B22
SSL2020 AIT Library Pass Thru with Transport	175312-B21

Add-on drives and accessories

SSL2020 AIT Library Pass Thru Extender	175312-B22
AIT 50GB Drive Add-On LVD Drive for SSL2020 AIT Library	175197-B21
19 Slot Magazine for SSL2020 AIT Library	175198-B21
AIT 50-GB Data Cassette (5 pack)	152841-001
AIT Cleaning Cassette	402374-B21

NOTE: Please see the SSL2020 Automated AIT Tape Library Solution QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10580_na/10580_na.HTML

StorageWorks MSL6000 and MSL5000 Departmental tape libraries

MSL6060L1 – Ultrium 460 1 based departmental library up to 4 drives and 60 slots

MSL6060L1, 0 DRV Ultrium 460 RM Library	331196-B23
MSL6060L1, 2 DRV Ultrium 460 RM Library	331195-B21
MSL6060L1, 2 DRV Ultrium 460 TT Library	331196-B21
MSL6060L1FC, 2 DRV Ultrium 460 embedded Fibre RM Library	331196-B22

NOTE: Please see the StorageWorks MSL6060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11608_na/11608_na.HTML

StorageWorks MSL6000 and MSL5000 departmental libraries

MSL5060L1 – LTO Ultrium 1 based departmental library up to 4 drives and 60 slots

MSL5060L1, 0 DRV LTO1 RM Library	301899-B21
MSL5060L1, 2 DRV LTO1 RM Library	301899-B22
MSL5060L1, 2 DRV LTO1 TT Library	301900-B21
MSL5060L1FC, 2 DRV LTO1 RM-with integrated FC router	301899-B23

NOTE: Please see the StorageWorks MSL5060 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11438_na/11438_na.HTML

MSL5052S2 – SDLT160 based departmental library up to 4 drives and 52 slots

MSL5052S2, RM 0 DRV SDLT ALL	255102-B21
MSL5052S2, 2 DRV SDLT2 TT LIB	293476-B21
MSL5052S2, 2 DRV SDLT2 RM LIB	293474-B21
MSL5052S2FC 2 DRV SDLT2 RM- with integrated FC router	293474-B24

NOTE: Please see the StorageWorks MSL5052S2 Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11442_na/11442_na.HTML

Options

MSL6030 – LTO Ultrium 460 mid-range library up to 2 drives and 30 slots	
MSL6030 0-drive, LTO, LVDS, RM	330731-B21
MSL6030 1-drive, LTO Gen2, LVDS, RM	330731-B22
MSL6030 2-drive, LTO Gen2, LVDS, RM	330731-B23
MSL6030 1-drive, LTO Gen2, Fibre, RM	330731-B24
MSL6030 2-drive, LTO Gen2, Fibre, RM	330731-B25
MSL6030 1-drive, LTO Gen2, LVDS, TT	330788-B21
MSL6030 2-drive, LTO Gen2, LVDS, TT	330788-B22
MSL5030L1 – LTO Ultrium 1 mid-range library up to 2 drives and 30 slots	
MSL5030L1, 0 DRV LTO1 RM Library	301897-B21
MSL5030L1, 1 DRV LTO1 RM Library	301897-B22
MSL5030L1, 2 DRV LTO1 RM Library	301897-B23
MSL5030L1, 1 DRV LTO1 TT Library	301898-B21
MSL5030L1, 2 DRV LTO1 TT Library	301898-B22
MSL5030L1FC, 1 DRV LTO1 RM- with integrated FC router	301897-B24

NOTE: Please see the StorageWorks MSL5030 LTO Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11439_na/11439_na.HTML

MSL5026S2 – SDLT160 based mid-range library up to 2 drives and 26 slots

MSL5026S2, 0 DRV SDLT2 RM Library	293472-B21
MSL5026S2, 1 DRV SDLT2 RM Library	293472-B22
MSL5026S2, 2 DRV SDLT2 RM Library	293472-B23
MSL5026S2, 1 DRV SDLT2 TT Library	293473-B21
MSL5026S2, 2 DRV SDLT2 TT Library	293473-B22
MSL5026S2FC, 1 DRV SDLT2 RM- with integrated FC router	293472-B24
MSL5026S2FC, 2 DRV SDLT2 RM- with integrated FC router	293472-B25

NOTE: Please see the StorageWorks MSL5026SL Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11453_na/11453_na.HTML

MSL5026SL Graphite – SDLT110 based mid-range library up to 2 drives and 26 slots

MSL5026SL, 1 DRV SDLT TT, graphite	302511-B21
MSL5026SL, 2 DRV SDLT TT, graphite	302511-B22
MSL5026SL, 1 DRV SDLT RM, graphite	302512-B21
MSL5026SL, 2 DRV SDLT RM, graphite	302512-B22

NOTE: Please see the StorageWorks MSL5026SL Graphite Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/11440_na/11440_na.HTML

MSL5026DLX– 40/80GB DLT based mid-range library up to 2 drives and 26 slots

MSL5026DLX, 1 40/80GB DLT, LVD, TT	231821-B21
MSL5026DLX, 2 40/80GB DLT, LVD, TT	231821-B22
MSL5026DLX, 1 40/80GB DLT, LVD, RM	231891-B21
MSL5026DLX, 2 40/80GB DLT, LVD, RM	231891-B22

NOTE: Please see the StorageWorks MSL5026DLX Library QuickSpecs for additional information including Upgrade Kits, Accessories, and SCSI Cable Kits and additional options needed for a complete solution at:
http://www5.compaq.com/products/quickspecs/10860_na/10860_na.HTML

MSL6000 and MSL5000 Add-on drives & accessories

MSL SDLT 160/320 Upgrade DRV	293475-B21
MSL Ultrium 460 upgrade drive in hot plug canister	330729-B21
MSL5000 SDLT 110/220 Upgrade DRV	231823-B22
MSL5000 40/80GB DLT Upgrade DRV	231823-B21
MSL Dual Magazine DLT (2 X 13 slot magazines)	232136-B21
MSL Universal passthrough mechanism	304825-B21
MSL 5U passthrough extender	231824-B22
MSL 10U passthrough extender	231824-B23
MSL Dual Magazine - Ultrium	301902-B21

Options

Smart Array Cluster Storage	Smart Array Cluster Storage	201724-B21
	Smart Array Cluster Storage Redundant Controller Option Kit	218252-B21
	128MB Cache Module for Smart Array 5302 Controller	153506-B21
	256MB Battery Backed Cache Module	254786-B21
	4-Port Shared Storage Module with Smart Array Multipath Software for Smart Array Cluster Storage	292944-B21
	NOTE: All 128MB Cache modules must be removed when 256MB cache modules are installed. NOTE: Please see the Smart Array Cluster Storage QuickSpecs for additional information including configuration steps and additional options needed for a complete solution at: http://www5.compaq.com/products/quickspecs/11050_na/11050_na.html	
External Storage – Tower and Rack	StorageWorks Enclosure Model 4314T (tower)	190210-001
	StorageWorks Enclosure Model 4314R (rack-mountable)	190209-001
	StorageWorks Enclosure Model 4354R (rack-mountable)	190211-001
	NOTE: The StorageWorks Enclosure 4300 Family support the Wide Ultra2/Ultra3 1" Hot Plug Hard Drives.	
	Redundant Power Supply Option	119826-B21
	Ultra3 Single Bus I/O Module Option	19021[illegible]
	Ultra3 Dual Bus I/O Module Option	190213-B21
	StorageWorks Enclosure Tower to Rack Conversion Kit	150213-B21
MSA1000	MSA1000	201723-B22
	MSA1000 Controller	218231-B22
	MSA Fibre Channel I/O Module	218960-B21
	MSA1000 Fabric Switch	218232-B21
	MSA1000 Fibre Channel Adapter (FCA) 2101	245299-B21
	HP StorageWorks msa hub 2/3	286763-B21
	NOTE: Please see the StorageWorks by Compaq Modular SAN Array 1000 QuickSpecs for additional options and configuration information at: http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML	
Network Storage Router	M2402 2FCX 4SCSI LVD Network Storage Router	262653-B21
	M2402 2FCX 4SCSI HVD Network Storage Router	262654-B21
	M2402 4 channel LVD SCSI Module	262659-B21
	M2402 4 channel HVD SCSI Module	26266[illegible]
	M2402 2 channel FC Module	262661-B21
	MSL5000 Embedded Router Fibre Option Kit - Graphite	262672-B21
	MSL5026 Embedded Router Fibre Option Kit - Opal	286694-B21
StorageWorks Options	StorageWorks Fibre Channel SAN Switches 8-EL	176219-B21
	StorageWorks SAN Switch 2/8-EL	258707-B21
	StorageWorks SAN Switch 2/16-EL	283056-B21
	StorageWorks SAN Switch 2/8-EL Upgrade Kit	288162-B21
	StorageWorks SAN Switch 2/16-EL Upgrade Kit	288250-B21

Options

UPS and PDU Power Cord Matrix	**Please see the UPS and PDU cable matrix that lists cable descriptions, requirements, and specifications for UPS and PDU units:** ftp://ftp.compaq.com/pub/products/servers/ProLiantstorage/power-protection/powercordmatrix.pdf. NOTE: This Web site is available in English only.	
Uninterruptible Power Systems – Tower UPSs	HP UPS Model T700 (700VA, 500 Watt), Low Voltage	204015-001
	HP UPS T1000 XR (1000 VA, 700 Watts), Low Voltage	204155-001
	HP UPS T1500 XR (1440 VA, 1050 Watts)	204155-002
	HP UPS T2200 XR (1920 VA, 1600 Watts) Low Voltage	204451-001
	HP UPS T2200 XR (2200 VA, 1600 Watts) High Voltage	204451-002
Uninterruptible Power Systems – HP Rack UPSs	HP UPS R1500 XR (100 to 127)	204404-001
	HP UPS R3000 XR (120V)	192186-001
	HP UPS R3000 XR (208V)	192186-002
	Rack-Mountable UPS R6000 (208V) NOTE: UPS R6000 has a hardwired input; and the UPS R12000 XR has a hardwired input and output connection.	347207-001
	HP UPS R12000 XR N+ x (200-240V) NOTE: The UPS R12000 XR has a hardwired input and output. NOTE: HP UPS R6000 has a hardwired input; the UPS R12000 XR has a hardwired input and output connection.	207552-B22
UPS Options	SNMP Serial Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 – 3000VA	192189-B21
	Six Port Card NOTE: Supports tower and rack UPS XR models ranging from 1000 – 3000VA.	192185-B21
	High to Low Voltage Transformer (250VA) NOTE: Supports R6000 UPS series only. 2.5A @ 125 Volts max output across two NEMA 5-15.	388643-B21
	Extended Runtime Module, T1000 XR	218967-B21
	Extended Runtime Module, T1500 XR/T2200 XR	218969-B21
	Extended Runtime Module, R1500 XR NOTE: 2U each, two ERM maximum.	218971-B21
	Extended Runtime Module, R3000 XR NOTE: 2U each, one ERM maximum.	192188-B21
	Extended Runtime Module, R6000 NOTE: 3U each, two ERM maximum.	347224-B21
	Extended Runtime Module, R12000 XR, 4U each, two ERMs maximum	217800-B21
	R12000 XR BackPlate Receptacle Kit, (2) L6-30R NOTE: The R12000 XR BackPlate Kit has a hardwired input.	325361-001
	R12000 XR BackPlate Receptacle Kit, (2) IEC-309R NOTE: The R12000 XR BackPlate Kit has a hardwired input.	325361-B21
	SNMP-EN Adapter NOTE: Supports R6000 UPS series only.	347225-B21
	Multi-Server UPS Card NOTE: Supports R6000 UPS series only.	123508-B21
	Scalable UPS Card NOTE: Supports R6000 UPS series only.	123509-B21

Options

Modular PDUs 1U/0U (Up to 32 outlets) NOTE: 1U/0U mounting brackets shipped with the unit (optimized for 10000 and 9000 series racks).	HP Modular Power Distribution Units (mPDU), Low Volt Model, 24A (100-127 VAC)	252663-D71
	NOTE: This mPDU (252663-D71) may also be used to connect the low volt model of the UPS R3000 XR.	
	HP Modular Power Distribution Units (mPDU), High Volt Model, 24A (200-240 VAC)	252663-D72
	HP Modular Power Distribution Units (mPDU), High Volt Model, 40A (200-240 VAC)	252663-B21
	NOTE: This mPDU (252663-B21), 40A model has a hardwired input.	
	HP Modular Power Distribution Units (mPDU), High Volt Model, 16A (200-240 VAC)	252663-B24
	NOTE: This PDU has a detachable input power cord and allows for adaptability to country specific power requirements. This model may also be used with the high volt UPSs R3000 XR and R6000. Order cable PN 340653-001.	
	NOTE: Please see the following Modular Power Distribution Unit (Zero-U/1U Modular PDUs) QuickSpecs for additional options including shorter jumper cables and country specific power cords: http://www5.compaq.com/products/quickspecs/11041_na/11041_na.HTML	
PDU Options	Third Party Modular PDU Modular Kit NOTE: This kit allows you to mount the Modular PDUs in (1U configuration only) in racks other than the 9000/10000 Series racks (any racks using the standard 19" rail, including the 7000 Series racks). For more details please refer the Modular PDU QuickSpecs.	310777-B21
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (1 per pack)	142257-006
	4.5' IEC C 13 to IEC C14 PDU Jumper Cable (15 per pack)	142257-007
USB Options	USB Easy Access Keyboard (carbon)	267146-008
	USB Easy Access Keyboard (carbonite)	DC168B#ABA
	USB 2-Button Scroll Mouse (carbon)	195255-B25
	USB 2-Button Scroll Mouse (carbonite)	DC172B
	USB Floppy	304707-B21
Other	Enhanced Keyboard (Carbon)	296435-005
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (HD68)	159547-B22
	ProLiant ML330/ML350 Internal to External SCSI Cable Option Kit (VHDCI) NOTE: The ProLiant ML330/ML350 Internal to External SCSI Cable Option Kits (PN 159547-B21 and 333370-B21) are supported by the ML330/ML350 Family.	333370-B21
Rack Builder	Please see the Rack Builder for configuration assistance at http://www.compaq.com/rackbuilder/	
Rack Conversion Kit	ProLiant ML350 Generation 3 Tower to Rack Conversion Kit (CPQ branded)	290683-B21

HP Rack 10000 Series (Graphite Metallic)	HP S10614 (14U) Rack Cabinet - Shock Pallet	292302-B22
	HP 10842 (42U) Rack Cabinet - Pallet	257415-B21
	HP 10842 (42U) Rack Cabinet - Shock Pallet	257415-B22
	HP 10647 (47U) – Pallet	245160-B21
	HP 10647 (47U) – Crated	245160-B23
	HP 10642 (42U) – Pallet	245161-B21
	HP 10642 (42U) – Shock Pallet	245161-B22
	HP 10642 (42U) – Crated	245161-B23
	HP 10636 (36U) – Pallet	245162-B21
	HP 10636 (36U) – Shock Pallet	245162-B22
	HP 10636 (36U) – Crated	245162-B23
	HP 10622 (22U) – Pallet	245163-B21
	HP 10622 (22U) – Shock Pallet	245163-B22
	HP 10622 (22U) – Crated	245163-B23

NOTE: -B21 (pallet) used to ship empty racks shipped on a truck
-B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels)
-B23 (crated) used for air shipments of empty racks

NOTE: It is mandatory to use a shock pallet in order to ship racks with equipment installed. Not all Compaq equipment is qualified to be shipped in the Rack 10000 series.

NOTE: Please see the Rack 10000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color:
http://www5.compaq.com/products/quickspecs/10995_na/10995_na.HTML

NOTE: For additional information regarding Rack Cabinets, please see the following URL:
http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html
NOTE: This Web site is available in English only.

Compaq Rack 9000 Series (opal)	Compaq Rack 9142 (42U) – Pallet	120663-B21
	Compaq Rack 9142 (42U) – Shock Pallet	120663-B22
	Compaq Rack 9142 (42U) – Crated	120663-B23

NOTE: –B21 (pallet) used to ship empty racks shipped on a truck
–B22 (shock pallet) used to ship racks with equipment installed (by custom systems, VARs and Channels)
–B23 (crated) used for air shipments of empty racks

NOTE: Please see the Rack 9000 QuickSpecs for Technical Specifications such as height, width, depth, weight, and color:
http://www5.compaq.com/products/quickspecs/10366_na/10366_na.HTML

NOTE: For additional information regarding Rack Cabinets, please see the following URL:
http://h18000.www1.hp.com/products/servers/proliantstorage/rack-ptions/index.html
NOTE: This Web site is available in English only.

Options

Rack Options for HP Rack 10000 Series	Rack Blanking Panels – Graphite (Multi)	253214-B26
	NOTE: Contains one each of 1U, 2U, 4U and 8U.	
	Rack Blanking Panels – Graphite (1U)	253214-B21
	NOTE: The Rack Blanking Panels (PN 253214-B21) contains 10 each of (1U).	
	Rack Blanking Panels – Graphite (2U)	253214-B22
	NOTE: The Rack Blanking Panels (PN 253214-B22) contains 10 each of (2U).	
	Rack Blanking Panels – Graphite (3U)	253214-B23
	NOTE: The Rack Blanking Panels (PN 253214-B23) contains 10 each of (3U).	
	Rack Blanking Panels – Graphite (4U)	253214-B24
	NOTE: The Rack Blanking Panels (PN 253214-B24) contains 10 each of (4U).	
	Rack Blanking Panels – Graphite (5U)	253214-B25
	NOTE: The Rack Blanking Panels (PN 253214-B25) contains 10 each of (5U).	
	600mm Stabilizer Kit – Graphite	246107-B21
	800mm Wide Stabilizer Kit (Graphite)	255488-B21
	NOTE: Supported by the Rack 10842 cabinet only.	
	Baying Kit for Rack 10000 series (Carbon)	24892
	42U Side Panel – Graphite Metallic	246099-B21
	110V Fan Kit (Graphite)	257413-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 5-15P.	
	220V Fan Kit (Graphite)	257414-B21
	NOTE: Roof Mount Includes power cord with IEC320-C13 to Nema 6-15P.	
	36U Side Panel – Graphite Metallic	246102-B21
	47U Side Panel – Graphite Metallic	255486-B21
	9000/10000 Series Offset Baying Kit (42U)	248931-B21
	NOTE: This kit can be used to connect 9000 and 10000 series racks of the same U height together. Kit contents include hardware for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	
	NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-ptions/index.html	
	NOTE: This Web site is available in English only.	

Rack Options for Compaq Rack 9000 Series	Baying/Coupling Kit	120669-B21
	42U Side Panel	120670-B21
	NOTE: The 42U Side Panel (PN 120670-B21) supports the Compaq Rack 9142 and Compaq Rack 9842.	
	36U Side Panel	120671-B21
	NOTE: The 36U Side Panel (PN 120671-B21) supports the Compaq Rack 9136.	
	600mm Stabilizer Option Kit	120673-B21
	800mm Stabilizer Option Kit (Opal)	234493-B21
	NOTE: The 800mm Stabilizer Kit (PN 234493-B21) supports the Rack 9842 only.	
	9142 Extension Kit	120679-B21
	NOTE: The 9142 Extension Kit (PN 120679-B21) supports the Compaq Rack 9142 only.	
	Stabilizer Option Kit	120673-B21
	Rack Blanking Panel Kit for Rack 9000 series (Opal) (U.S.) NOTE: The Rack Blanking Panel Kit (PN 169940-B21) contains 4 panels – one each of 1U, 2U, 4U and 8U.	169940-B21
	Rack Blanking Panels (1U) NOTE: The Rack Blanking Panels (PN 189453-B21) contains 10 each of (1U).	189453-B21
	Rack Blanking Panels (2U) NOTE: The Rack Blanking Panels (PN 189453-B22) contains 10 each of (2U).	189453-B22
	Rack Blanking Panels (3U) NOTE: The Rack Blanking Panels (PN 189453-B23) contains 10 each of (3U).	189453-B23
	Rack Blanking Panels (4U) NOTE: The Rack Blanking Panels (PN 189453-B24) contains 10 each of (4U).	189453-B24
	Rack Blanking Panels (5U) NOTE: The Rack Blanking Panels (PN 189453-B25) contains 10 each of (5U)	189453-B25
	9136 Extension Kit	218216-B21
	9142 Short Rear Door NOTE: The 9142 Short Rear Door (PN 218217-B21) supports the Compaq Rack 9142 only.	218217-B21
	Split Rear Door (Opal) NOTE: The Split Rear Door (PN 254045-B21) supports the 600 mm wide, 42U 9000 series rack.	254045-B21
	9136 Short Rear Door	218218-B21
	9142 Split Rear Door	254045-B21
	9000/10000 Offset Baying Kit (42U) NOTE: This kit can be used to connect 9000 and 10000 series racks of same U height together. Kit contents include hardware for connecting racks and a panel to cover the 100mm gap at the rear of the two racks.	248931-B21
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	

Rack Options for Compaq Rack 7000 Series	High Air Flow Rack Door Insert for the 7122 Rack	157847-B21
	High Air Flow Rack Door Insert for the 7142 Rack (single)	327281-B21
	High Air Flow Rack Door Insert for the 7142 Rack (6-pack)	327281-B22
	Compaq Networking Cable Management Kit	292407-B21
	Compaq Rack Extension Kit for 7142	154392-B21
	NOTE: For additional information regarding Rack Cabinets, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html NOTE: This Web site is available in English only.	

Options

Rack Options for Rack 7000, 9000 and 10000 Series

Monitor Utility Shelf	303606-B21
Ballast Option Kit	120672-B21
100kg Sliding Shelf	234672-B21
Rack Rail Adapter Kit (25-inch depth)	120675-B21
Cable Management D-Rings Kit	168233-B21
Console Management Controller (CMC) Option Kit	203039-B21
Console Management Controller (CMC) Sensors Option Kit	203039-B22
Console Management Controller (CMC) Locking Option Kit	203039-B23
Console Management Controller (CMC) Smoke Sensors Option Kit	203039-B24
Server Console Switch 1 x 2 port (100 to 230 VAC)	120206-001
Server Console Switch 1 x 4 port (100 to 230 VAC)	400336-001
Server Console Switch 1 x 8 port (100 to 230 VAC)	400337-001
Server Console Switch 2 x 8 port (100 to 230 VAC)	400338-001
Server Console Switch 2 x 8 port (48 VDC)	400542-B21
IP Console Switch Box, 1x1x16	262585-B21
IP Console Switch Box, 3x1x16	26258
IP Console Interface Adapter, 8 pack	262587-B21
IP Console Interface Adapter, 1 pack	262588-B21
IP Console Expansion Module	262589-B21
KVM 9 PIN Adapter (4 Pack)	149361-B21
CPU to Server Console Cable, 12'	110936-B21
CPU to Server Console Cable, 20'	110936-B22
CPU to Server Console Cable, 40'	110936-B23
CPU to Server Console Cable, 3'	110936-B24
CPU to Server Console Cable, 7'	110936-B25
CPU to Server Console Cable (Plenum Rated) 20'	149363-B21
CPU to Server Console Cable (Plenum Rated) 40'	149364-B21
IP CAT5 Cable 3', 4 pack	263474-B21
IP CAT5 Cable 6', 8 pack	263474-B22
IP CAT5 Cable 12', 8 pack	263474-B23
IP CAT5 Cable 20', 4 pack	263474-B24
IP CAT5 Cable 40', 1 pack	263474-B25
Switch Box Connector Kit (115 V)	144007-001
Switch Box Connector Kit (230 V)	14400
1U Rack Keyboard & Drawer (Carbon)	257054-001
NOTE: The 1U Rack Keyboard & Drawer (PN 257054-001) is to be used with the Keyboards for Racks with Trackball (PN 158649-001).	
TFT5600 Rack Keyboard Monitor	221546-001
Input Device Adjustable Rails	287139-B21
NOTE: Input Device Adjustable Rails (287139-B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	
Input Device Telco Rail	287138-B21
NOTE: Input Device Telco Rails (287138-B21) are for use ONLY with the TFT5110R, TFT5600RKM and integrated keyboard/drawer which is used in mounting into third party racks.	
Keyboard/Monitor/Mouse extension cables	169989-001

NOTE: For additional information regarding Rack Options, please see the following URL: http://h18000.www1.hp.com/products/servers/proliantstorage/rack-options/index.html

NOTE: This Web site is available in English only

When routes are created, they are injected into any dynamic routing protocol and distributed to surrounding devices. This traffic flows, requiring IPSec to be directed to the appropriate RRI router for transport across the correct SAs to avoid IPSec policy mismatches and possible packet loss.

Hot Standby Router Protocol and IPSec

Hot Standby Router Protocol (HSRP) is designed to provide high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. HSRP is particularly useful for hosts that do not support a router discovery protocol, such as ICMP Router Discovery Protocol (IRDP), and do not have the functionality to switch to a new router when their selected router reloads or loses power. Without this functionality, a router that loses its default gateway because of a router failure is unable to communicate with the network.

HSRP is configurable on LAN interfaces using standby command line interface (CLI) commands. It is now possible to use the standby IP address from an interface as the local IPSec identity, or local tunnel endpoint.

By using the standby IP address as the tunnel endpoint, failover can be applied to VPN routers by using HSRP. Remote VPN gateways connect to the local VPN router via the standby address that belongs to the active device in the HSRP group. In the event of failover, the standby device takes over ownership of the standby IP address and begins to service remote VPN gateways.

Further Documentation

Refer to the following document for further information about the IPSec VPN High Availability Enhancements feature:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e9/ipsecha.htm.

Large-Scale Dial-Out (LSDO) VRF Aware

The Large-Scale Dial-Out (LSDO) VRF Aware feature allows LSDO to support the Layer 2 Tunnel Protocol (L2TP) in an Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN). The basic operation of LSDO relies on per-user static routes stored in an authentication, authorization, and accounting (AAA) server and redistributed static routes and redistributed connected routes to put better routes that point to the same remote network or host on the alternate network access server (NAS). When using LSDO, overlapping IP addresses are often present in virtual routing and forwarding instances (VRFs), so that a unique key is needed to retrieve the correct route from the AAA server. With virtual private dial network (VPDN) as a dial-out resource, a virtual access interface is created for maintaining each PPP session. Software before Cisco IOS Release 12.2(8)T did not update the VRF information on the virtual access interface; rather, this information was cloned from the dialer interface. Now, the VRF table identifier is retrieved from the incoming packet and is mapped to the VRF name. This VRF name and the destination IP address are combined to make the unique key needed to retrieve the dial string and other user profile information from the AAA server.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftlsdvpn.htm.

Media Gateway Control Protocol Based Fax (T.38) and Dual Tone Multifrequency (IETF RFC 2833) Relay

The MGCP-Based Fax (T.38) and DTMF (IETF RFC 2833) Relay feature adds support for fax relay and DTMF relay with MGCP. This feature provides two modes of implementation for each component: gateway (GW) controlled mode and call agent (CA) controlled mode. In GW controlled mode, GWs negotiate DTMF and fax relay transmission by exchanging capability information in Session Definition Protocol (SDP) messages. That transmission is transparent to the CA. GW-controlled mode allows use of the MGCP-Based Fax (T.38) and DTMF (IETF RFC 2833) Relay feature without upgrading the CA software to support the feature. In CA-controlled mode, CAs use MGCP messaging to instruct GWs to process fax and DTMF traffic. For MGCP T.38 Fax Relay, the CAs can also instruct GWs to revert to GW-controlled mode if the CA is unable to handle the fax control messaging traffic; for example, in overloaded or congested networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmgcpfx.htm.

MGCP VoIP Call Admission Control

MGCP CAC determines if calls can be accepted on the IP network on the basis of available network resources. Before this release, MGCP Voice over IP (VoIP) calls were established regardless of the available resources on the gateway or network. The gateway had no mechanism for gracefully refusing calls if resources were not available to process the call. New calls would fail with unexpected behavior and in-progress calls would experience quality-related problems.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_04mac.htm.

MPLS Label Distribution Protocol (LDP)

Cisco MPLS label distribution protocol (LDP) allows the construction of highly scalable and flexible IP Virtual Private Networks (VPNs) that support multiple levels of services.

LDP provides a standard methodology for hop-by-hop distribution of labels in an Multiprotocol Label Switching (MPLS) network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting label switch paths (LSPs) forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement Cisco MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ldp7t.htm.

MPLS Over ATM: Virtual Circuit (VC) Merge

VC merge maps several incoming labels to one single outgoing label. Cells from different virtual channel identifiers (VCIs) that travel to the same destination are transmitted to the same outgoing VC using multipoint-to-point connections.

VC merge allows the switch to transmit cells that come from different VCIs over the same outgoing VCI to the same destination. In other words, VC merge queues ATM Adaptation Layer 5 (AAL5) frames in input buffers until the switch receives the last frame. Then the switch transmits the cells from that AAL5 frame before it sends any cells from other frames. VC merge requires the switch to provide buffering, but no more buffering than is required in IP networks. VC merge slightly delays the transfer of frames; however, VC merge is for IP traffic and not for traffic that requires speed. IP traffic tolerates delays better than other traffic on the ATM network.

MPLS Traffic Engineering (TE) MIB

Simple Network Management Protocol (SNMP) agent code operating in conjunction with the MPLS Traffic Engineering MIB (MPLS TE MIB) enables a standardized, SNMP-based approach to be used in managing the Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) features in Cisco IOS software.

The MPLS TE MIB is based on the Internet Engineering Task Force (IETF) draft MIB entitled draft-ietf-mpls-te-mib-05.txt, which includes objects describing features that support MPLS traffic engineering. This IETF draft MIB, which undergoes revisions from time to time, is being evolved toward becoming a standard. Accordingly, Cisco's implementation of the MPLS TE MIB is expected to track the evolution of the IETF draft MIB.

The SNMP objects defined in the MPLS TE MIB can be viewed by any standard SNMP utility. All MPLS TE MIB objects are based on the IETF draft MIB; thus, no specific Cisco SNMP application is required to support the functions and operations pertaining to the MPLS TE MIB.

The MPLS TE MIB provides the following benefits:

- Provides a standards-based SNMP interface for retrieving information about MPLS traffic engineering.
- Provides information about the traffic flows on MPLS traffic engineering tunnels.
- Presents MPLS traffic engineering tunnel routes, including the configured route, the IGP calculated route, and the actual route traversed.
- Provides information, in conjunction with the Interfaces MIB, about how a tunnel was rerouted in the event of a link failure.
- Provides information about the configured resources used for an MPLS traffic engineering tunnel.
- Supports the generation and queueing of notifications that call attention to major changes in the operational status of MPLS traffic engineering tunnels; forwards notification messages to a designated network management station (NMS) for evaluation/action by network administrators.

Refer to the following document for additional information.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/temib28t.htm.

MPLS VPN Carrier Supporting Carrier

The carrier supporting carrier feature enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftcsc8.htm.

Note This document focuses on a backbone carrier that offers Border Gateway Protocol and Multiprotocol Label Switching (BGP/MPLS) VPN services.

MPLS VPN ID

Using Multiprotocol Label Switching (MPLS) VPN ID you can identify virtual private networks (VPNs) by a VPN identification number, as described in RFC 2685. This implementation of the MPLS VPN ID feature is used for identifying a VPN. The MPLS VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with MPLS VPN ID numbers in routing updates.

Multiple VPNs can be configured in a router. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the router. Alternately, you can use a VPN ID to identify a particular VPN in the router. The VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the routers in the service provider network that services that VPN.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftvpnid.htm.

Multilink Frame Relay

The Multilink Frame Relay feature introduces functionality based on the Frame Relay Forum Multilink Frame Relay UNI/NNI Implementation Agreement (FRF.16). This feature provides a cost-effective way to increase bandwidth for particular applications by enabling multiple serial links to be aggregated into a single bundle of bandwidth. Multilink Frame Relay is supported on User-to-Network Interfaces (UNIs) and Network-to-Network Interfaces (NNIs) in Frame Relay networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_mfr.htm.

Multiple RSA Key Pair Support

The Multiple RSA Key Pair Support feature allows the Cisco IOS software to maintain a distinct key pair for each certification authority (CA) with which it is dealing. Thus, the Cisco IOS software can match policy requirements for each CA without compromising the requirements specified by the other CAs, such as key length, key lifetime, and general-purpose versus special-usage keys.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmltkey.htm.

Multiprotocol BGP (MP-BGP) Support for CLNS

The Multiprotocol BGP Support for CLNS feature allows Border Gateway Protocol (BGP) to be used as an interdomain routing protocol in networks that use Connectionless Network Service (CLNS) as the network-layer protocol. This feature was developed to solve a scaling issue with a data communications network (DCN) where large numbers of routers are managed remotely. The benefits of using Multiprotocol BGP (MP-BGP) to support CLNS are not confined to DCN networks and can be implemented to help scale any network using Open System Interconnection (OSI) routing protocols with CLNS.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fm_bgpmc.htm.

NAT Support for SIP

The Session Initiation Protocol (SIP) is an application layer signaling protocol used for creating and controlling multimedia sessions with two or more participants. SIP is transported over TCP or UDP. The messages used in the protocol may have IP addresses embedded in the packet payload. If a message passes through a router configured with Network Address Translation (NAT), the embedded information must be translated and encoded back to the packet. An Application Layer Gateway (ALG) is used with NAT to enable SIP.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftnatsip.htm.

Network-Based Application Recognition RTP Payload Type Classification

The RTP Payload Type Classification enhancement has been added to the Network-Based Application Recognition (NBAR) feature. With the addition of NBAR RTP Payload Type Classification, RTP traffic can now be classified as a protocol within the Modular QoS CLI framework.

For additional information on the NBAR feature, including NBAR RTP Payload Type Classification, refer to the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm.

Nonstop Forwarding Enhanced FIB Refresh

Operational networks must minimize traffic disruption and offer the most uptime possible. The Nonstop Forwarding Enhanced FIB Refresh feature provides users the capability to continue forwarding IP traffic while Cisco Express Forwarding (CEF) database tables are being rebuilt. IP forwarding on the router is therefore uninterrupted.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftfibeps.htm.

OSPF Sham-Link Support for MPLS VPN

A sham link is a logical path within an Open Shortest Path First (OSPF) area; it represents an unnumbered point-to-point connection between two provider edge (PE) devices. All routers within the area see the link and use it during the shortest path first (SPF) computation.

On PE routers the VPN Route Forwarding (VRF) routing table is populated by OSPF routes over the sham link. The sham link gives users the capability of specifying which path will be used for traffic.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ospfshmk.htm

PIM Multicast Scalability

This feature enhances the Protocol Independent Multicast (PIM) protocol in Cisco IOS software by adding a new level of scalability. With this feature, edge devices can have a large number of multicast groups and users without increasing the CPU utilization of the router.

Plain NFAS Support on NM-HDV

The current Non-Facility Associated Signaling (NFAS) support on the High-Density Voice network modules (NM-HDV) is joined with the Redundant Link Manager/Signaling System 7 (RLM/SS7). When a user configures an ISDN PRI NFAS group via the Cisco command line interface (CLI), all channels within the PRI are treated as B channels. A D channel is not created and, thus no signaling will be passed to the ISDN stack.

This feature modifies the existing implementation of NFAS/RLM on NM-HDV to activate the generic NFAS feature on Cisco 2600 and 3600 routers and to allow the coexistence of plain NFAS and NFAS/RLM/SS7 on the Cisco 3660 router.

Policer Enhancement—Multiple Actions

This feature further extends the functionality of the Cisco IOS Traffic Policing feature (a single-rate policer) and the Two-Rate Policer feature. The Traffic Policing and Two-Rate Policer features are traffic policing mechanisms that allow you to control the maximum rate of traffic sent or received on an interface. Both of these traffic policing mechanisms mark packets as conforming to, exceeding, or violating a specified rate. After a packet is marked, you can specify an action to be taken on the pack on the basis of that marking.

With both the Traffic Policing feature and the Two-Rate Policer feature, you can specify only one conform action, one exceed action, and one violate action. Now with the new Policer Enhancement—Multiple Actions feature, you can specify multiple conform, exceed, and violate actions for the marked packets. You specify the multiple actions by using the action argument of the police command.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftpolenh.htm.

PPPoE MTU Adjustment

The syntax of the **ip adjust-mss** command has changed to the following:

ip tcp adjust-mss *mss*

where the value of the *mss* argument must be 1452 or less to fix the Point-to-Point Protocol over Ethernet (PPPoE) maximum transmission unit (MTU) problem.

PPPoE Session-Count MIB

The PPPoE Session-Count MIB provides the ability to use Simple Network Management Protocol (SNMP) to monitor in real time the number of PPP over Ethernet sessions configured on permanent virtual circuits (PVCs) and on a router.

This new MIB also introduces two SNMP traps that generate notification messages when a PPPoE session-count threshold is reached on any PVC or on the router.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftpscmib.htm.

Radius Packet of Disconnect

This feature consists of a method for terminating a call that has already been connected. The "Packet of Disconnect" (POD) is a RADIUS access_request packet and is intended to be used in situations in which the authenticating agent server wants to disconnect the user after the session has been accepted by the RADIUS access_accept packet. This may be needed in at least two situations:

- Detection of fraudulent use, which cannot be performed before accepting the call, or a price structure so complex that the maximum session duration cannot be estimated before accepting the call. This may be the case when certain types of discounts are applied or when multiple users use the same subscription simultaneously.
- To prevent unauthorized servers from disconnecting users, the authorizing agent that issues the POD packet must include three parameters in its packet of disconnect request. For a call to be disconnected, all parameters must match their expected values at the gateway. If the parameters do not match, the gateway discards the packet of disconnect packet and sends a NACK (negative acknowledgement message) to the agent.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_pod1.htm.

RADIUS Route Download

The RADIUS Route Download feature allows users to configure their network access server (NAS) to send static route download requests to authentication, authorization, and accounting (AAA) servers specified by a named method list. Before this feature, all RADIUS authorization requests for static route download could be sent only to AAA servers specified by the default method list.

This feature extends the functionality of the **aaa route download** command to allow users to specify the name of the method list that will be used to direct static route download requests to the AAA servers. The **aaa route download** command must be used to add separate method lists; however, users will continue to enable the **aaa authorization configuration default** command to download static route configuration information from the AAA server specified by the default method list.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftradrou.htm.

Rotating Through Dial Strings

The Rotating Through Dial Strings feature allows you to specify the dialing order when multiple dial strings are configured. Options for dialing order include:

- Sequential—Dial using the first dial string configured in a list of multiple strings.
- Round-robin—Dial using the dial string following the most recently successful dial string.
- Last successful call—Dial using the most recently successful dial string.

This feature takes advantage of information available from a previous call attempt, such as whether the call was unsuccessful or the line was busy, and thereby increases the rate of successful calls.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftrotdls.htm.

Secure Shell (SSH) Support over IPv6

Secure Shell (SSH) in IPv6 functions the same and offers the same benefits as SSH in IPv4—the SSH Server feature enables an SSH client to make a secure, encrypted connection to a Cisco router, and the SSH Client feature enables a Cisco router to make a secure, encrypted connection to another Cisco router or to any other device that is running an SSH server. IPv6 enhancements to SSH consist of support for IPv6 addresses that enable a Cisco router to accept and establish secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/index.htm.

Secure Shell (SSH) Version 1 Server Support

Secure Shell (SSH) is an application and a protocol that provide a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used much like the Berkeley rexec and rsh tools are used. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software. For more information on this feature, refer to the "Configuring Secure Shell" chapter of the *Cisco IOS Security Configuration Guide*, Release 12.2.

This feature was originally introduced in Cisco IOS Release 12.1(1)T. This release adds support for the Cisco 826, Cisco 827, and Cisco 827-4V platforms.

Service Selection Gateway

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as digital subscriber lines, cable modems, or wireless to allow simultaneous access to network services.

SSG works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM).

Together with the SSD or SESM, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services.

Subscribers interact with an SSD or SESM web application using a standard Internet browser.

SSG communicates with the authentication, authorization, and accounting (AAA) management network where RADIUS, Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of SSG works with SESM to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This functionality improves flexibility and convenience for subscribers and enables service providers to bill subscribers for connect time and services used, rather than charging a flat rate.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/ft_ssg.htm.

Session Initiation Protocol (SIP) for VoIP

Voice over IP (VoIP) currently implements the ITU H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. Session Initiation Protocol (SIP) is a protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to H.323. The Cisco SIP functionality equips Cisco routers to signal the setup of voice and multimedia calls over IP networks. SIP provides an alternative to H.323 within the VoIP internetworking software.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_sip72.htm.

Simple Network-Enabled Auto-Provisioning for Cisco IAD2420 Series IADs

The Simple Network-Enabled Auto-Provisioning (SNAP) feature on the Cisco IAD2420 series IAD allows service providers to rapidly deploy and configure services to the Cisco IAD platforms at customer premises without requiring configuration of the IADs at the customer site and with little or no onsite technician intervention. SNAP is part of the Cisco Networking Services (CNS) technology, which allows network products to be installed and automates many of the configuration tasks. SNAP consists of two basic functions: learning and setting the IP address and downloading the configuration for the IAD.

Each Cisco IAD2420 series IAD using SNAP includes a CNS Configuration Agent and CNS Event Agent that communicates with the CNS Configuration Registrar to enable the configuration of the IAD.

Using SNAP in conjunction with a Cisco aggregation router, a CNS Configuration Registrar, and an optional Domain Name System (DNS) server, SNAP performs the IAD configuration on the CNS Configuration Registrar and downloads the configuration to the IAD at the customer premises.

SIP Gateway Support for the Bind Command

In previous releases of Cisco IOS software, the source address of a packet going out of the gateway was never deterministic. That is, the session protocols and Voice over IP (VoIP) layers always depended on the IP layer to give the *best local address*. The best local address was then used as the source address (the address showing where the SIP request came from) for signaling and media packets. Using this nondeterministic address occasionally caused confusion for firewall applications, because a firewall could not be configured with an exact address and would take action on several different source address packets.

However, the bind interface command allows you to configure the source IP address of signaling and media packets to a specific interface's IP address. Thus, the address that goes out on the packet is bound to the IP address of the interface specified with the bind command. Packets that are not destined to the bound address are discarded.

When you do not want to specify a bind address, or if the interface is down, the IP layer still provides the best local address.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftbind.htm.

SIP Gateway Support of RSVP and TEL URL

The SIP Gateway Support of RSVP and TEL URL feature also supports Telephone Uniform Resource Locators or TEL URL. Currently SIP gateways support URLs in the SIP format. SIP URLs are used in SIP messages to indicate the originator, recipient, and destination of the SIP request. However, SIP gateways may also encounter URLs in other formats, such as TEL URLs. TEL URLs describe voice call connections. They also enable the gateway to accept TEL calls sent through the Internet and to generate TEL URLs in the request line of outgoing INVITE requests.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/vvfresrv.htm.

SIP Intra-gateway Hairpinning

SIP hairpinning is a call routing capability in which an incoming call on a specific gateway is signaled through the IP network and back out the same gateway. This call can be a public switched telephone network (PSTN) call routed into the IP network and back out to the PSTN over the same gateway.

Similarly, SIP hairpinning can be a call signaled from a line (for example, a telephone line) to the IP network and back out to a line on the same access gateway. With SIP hairpinning, unique gateways for ingress and egress are no longer necessary.

SIP INVITE Request with Malformed Via Header

A SIP INVITE requests that a user or service participate in a session. Each INVITE contains a Via header that indicates the transport path taken by the request so far and where to send a response.

In the past, when an INVITE contained a malformed Via header, the gateway would print a debug message and discard the INVITE without incrementing a counter. However, the printed debug message was often inadequate, and it was difficult to detect that messages were being discarded.

The SIP INVITE Request with Malformed Via Header feature provides a response to the malformed request. A counter, *Client Error: Bad Request,* increments when a response is sent for a malformed Via field. *Bad Request* is a class 400 response and includes the explanation *Malformed Via Field.* The response is sent to the source IP address (the IP address where the SIP request originated) at User Datagram Protocol (UDP) port 5060.

This feature applies to messages arriving on UDP, because the Via header is not used to respond to messages arriving on TCP.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmalvia.htm.

SIP T.37 Store and Forward Fax

SIP T.37 is an ITU specification that enables store-and-forward fax applications, as well as toggling from voice to fax, for example, providing an Interactive Voice Response (IVR) front end to a store-and-forward fax application.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/index.htm

SIP T.38 Fax Relay

The SIP T.38 Fax Relay feature adds standards-based fax support to Session Initiation Protocol (SIP) and conforms to ITU-T T.38, *Procedures for Real-Time Group 3 Facsimile Communication over IP Networks*. The ITU-T standard specifies real-time transmission of faxes between two regular fax terminals over an IP network.

The SIP T.38 Fax Relay feature also includes the following functionality:

- Support for Facsimile User Datagram Protocol Transport Layer (UDPTL)

  UDPTL, as defined in ITU-T T.38, is a transport layer that is used on top of UDP. UDPTL makes the delivery of packets more reliable by providing data redundancy.

- Support for quality of service (QoS)

  SIP T.38 Fax Relay supports QoS when establishing T.38 sessions. If the dial peer is already configured for QoS, the T.38 stream maintains the QoS support. QoS ensures certain bandwidth reservations for calls.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftsipfax.htm.

SIP—Call Transfer Using Refer Method

Note The SIP—Call Transfer Using Refer Method feature is also known under the feature title Call Transfer Capabilities Using the Refer Method.

The Refer method provides call transfer capabilities to supplement the Bye and Also methods already implemented on Cisco IOS Session Initiation Protocol (SIP) gateways.

Call transfer allows a wide variety of decentralized multiparty call operations. These decentralized call operations form the basis for third-party call control and thus are important features for Voice over IP (VoIP) and SIP. Call transfer is also critical for conference calling, where calls can transition smoothly between multiple point-to-point links and IP level multicasting.

The following are components of call transfer:

- Refer Method
- Refer-To Header
- Referred-By Header
- Notify Method
- Using the Refer Method to Achieve Call TransferBlind Transfer
- Attended Transfer

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftrefer.htm.

SIP—DNS SRV RFC2782 Compliance

Session Initiation Protocol (SIP) on Cisco Voice over IP (VoIP) gateways uses Domain Name System Server (DNS SRV) query to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." and is attached to the fully qualified domain name (FQDN) of the next hop SIP server. This prefix style, from RFC 2052, has always been available; however, with this release, a second style is also available. The second style complies with RFC 2782 and prepends the protocol label with an underscore "_"; as in "_protocol._transport." The addition of the underscore reduces the risk of the same name being used for unrelated purposes. The form compliant with RFC 2782 is the default style. Use the **srv version** command to configure the DNS SRV feature.

SNMP IF-MIB Support for VLAN (ISL, 802.1Q) Subinterfaces

This feature updates the Cisco implementation of the Interfaces Group MIB (abbreviated "IF-MIB" and defined in RFC 2233) to completely support ifTable and ifXTable entries for Inter-Switch Link (ISL) or 802.1Q encapsulated subinterfaces.

The Interface Table (the ifTable object) contains information on an Simple Network Management Protocol (SNMP) management entity's interfaces. Each sublayer of a network interface is considered t be an interface. An ifTable is a list of interface entries in which each entry contains management information applicable to that interface. The ifXTable is an extension to the ifTable. It contains replacements for objects of the ifTable that were deprecated. The ifXTable also contains 64-bit versions of the counters defined in the ifTable. Cisco IOS software can support both interfaces and subinterfaces in the ifTable.

ISL is a Cisco protocol for interconnecting switches and maintaining VLAN information as traffic is exchanged between switches. It can also be used to configure routing between any number of VLANs in a network by creating subinterfaces for each VLAN.

802.1Q (also referred to as "DOT1Q") is an IEEE standard protocol for interconnecting bridges/switches and maintaining VLAN information as traffic is exchanged between the devices. 802.1Q can also be used to configure routing between any number of VLANs in a network by creating subinterfaces for each VLAN.

The following objects of the ifTable have been updated: ifIndex, ifDescr, ifType, ifMtu, ifSpeed, ifPhysAddress, ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts.

The following objects of the ifXTable have been updated: ifName, ifInMulticastPkts, ifInBroadcastPkts, ifOutMulticastPkts, ifOutBroadcastPkts, ifHCInOctets, ifHCInUcastPkts, ifHCInMulticastPkts, ifHCInBroadcastPkts, ifHCOutOctets, ifHCOutUcastPkts, ifHCOutMulticastPkts, ifHCOutBroadcastPkts.

Static Cache Entry for IPv6 Neighbor Discovery

The Static Cache Entry for IPv6 Neighbor Discovery feature enables the configuring of static entries in the IPv6 neighbor discovery cache, which provides functionality in IPv6 that is equivalent to static Address Resolution Protocol (ARP) entries in IPv4. Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process. Cisco IOS software uses static ARP entries in IPv4 to translate 32-bit IP addresses into 48-bit hardware addresses. In IPv6, Cisco IOS software uses static entries in the IPv6 neighbor discovery cache to translate 128-bit IPv6 addresses into 48-bit hardware addresses.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/ftipv6s.htm.

Stream Control Transmission Protocol (SCTP) Release 2

Stream Control Transmission Protocol (SCTP) is a reliable datagram-oriented IP transport protocol specified by RFC 2960. It provides the layer between an SCTP user application and an unreliable end-to-end datagram service such as IP. The basic service offered by SCTP is the reliable transfer of user datagrams between peer SCTP users. It performs this service within the context of an association between two SCTP hosts. SCTP is connection-oriented, but SCTP association is a broader concept than the TCP connection, for example.

SCTP is not explicitly configured on routers, but it underlies several Cisco applications. The commands described in the document referenced below are useful for troubleshooting when SCTP issues are suspected as the cause of problems.

The SCTP feature was originally introduced in Cisco IOS Release 12.2(4)T as Release 1. SCTP Release 2 includes updated output for the **show ip sctp association parameters** and **show ip sctp association statistics** commands.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_sctp2.htm.

Survivable Remote Site Telephony Version 1.0

The Survivable Remote Site (SRS) Telephony feature, under the IP Telephony services umbrella, provides the Cisco CallManager with fallback support for the Cisco IP phones attached to the Cisco router on your local Ethernet. The SRS Telephony feature enables the routers to provide call handling support for the Cisco IP phones when the Cisco IP phones lose connection to the remote primary, secondary, or tertiary Cisco CallManager or when the WAN connection is down.

Survivable Remote Site Telephony Version 2.0

The Survivable Remote Site (SRS) Telephony feature, under the IP Telephony services umbrella, provides the Cisco CallManager with fallback support for the Cisco IP phones attached to the Cisco router on your local Ethernet. The SRS Telephony feature enables the routers to provide call handling support for the Cisco IP phones when the Cisco IP phones lose connection to the remote primary, secondary, or tertiary Cisco CallManager or when the WAN connection is down.

Cisco CallManager 3.0 supports Cisco IP phones at remote sites attached to Cisco branch office multiservice routers across the WAN. Prior to the SRS Telephony feature, when the WAN connection between the remote branch office router and the Cisco CallManager failed or connectivity with the Cisco CallManager was lost for some reason, the Cisco IP phones at the branch office became unusable for the duration of the failure. The SRS Telephony feature overcomes this problem and enables the basic features of the Cisco IP phones by providing call-handling support on the branch office router for its attached Cisco IP phones. The system automatically detects the failure and uses the Simple Network Auto Provisioning (SNAP) technology to autoconfigure the branch office router to provide call processing for the local Cisco IP phones. When the WAN link or connection to the primary Cisco CallManager is restored, call-handling capabilities for the Cisco IP phones switch back to the primary Cisco CallManager. During a failure when SRS Telephony feature is enabled, the Cisco IP phone displays a message to inform you that the Cisco IP phones are in the Cisco CallManager fallback mode and are able to perform limited functions.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/srs/fallbak2.htm.

T.37 Store-and-Forward Fax for Cisco 1751 Modular Access Routers

Fax applications enable Cisco 1751 modular access routers to send and receive faxes across packet-based networks by using voice interface cards (VICs) that support Foreign Exchange Station (FXS), Foreign Exchange Office (FXO), Ear and Mouth (E&M), and BRI NT/TE signaling protocols.

The Cisco 1751 modular access routers support carrier-class Voice over IP (VoIP) and fax over IP services. Because the Cisco 1751 modular access routers are H.323 compliant, they support a family of industry-standard voice codecs and provide echo cancellation and voice activity detection (VAD) and silence suppression. There is an interactive voice response (IVR) application that provides voice prompts and digit collection in order to authenticate the user and identify the call destination.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/plfxrl17.htm.

T.37 Store-and-Forward Fax for the Cisco 2600 Series and Cisco 3600 Series Routers

This feature adds fax detection and store and forward fax to the Cisco 2600 series and Cisco 3600 series routers. When equipped with digital and analog voice network modules, these routers support configuration of the T.37/T38 fax gateway. Supported network modules are NM-HDV with voice interface cards (VICs) for digital T1 connections and Voice 2V with VICs FXS for analog connections. VWIC and VIC FXS are the voice interface cards within the network modules.

Voice network modules installed in Cisco 2600 series or Cisco 3600 series routers convert telephone voice signals into data packets that can be transmitted over an IP network. VWICs/VICs work with existing telephone and fax equipment and are compatible with H.323 standards for audio and video conferencing.

Cisco 2600 series and Cisco 3600 series routers that support carrier-class Voice over IP (VoIP) and fax over IP services provide echo cancellation and voice activity detection (VAD)/silence suppression. An interactive voice response (IVR) application provides voice prompts and digit collection to authenticate the user and identify the call destination.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/plfxrl17.htm.

TCP Window Scaling

TCP Window Scaling adds support for the Window Scaling extension option in RFC 1323. To improve TCP performance in network paths with a large bandwidth-delay product, Long Fat Networks (LFNs), a larger window size is recommended. This TCP Window Scaling enhancement provides that support.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/tcpwslfn.htm.

Trustpoint CLI

The Trustpoint CLI feature introduces the **crypto ca trustpoint** command, which combines and replaces the functionality of the existing **crypto ca identity** and **crypto ca trusted-root** commands.

Although both of the existing commands allow you to declare the certification authority (CA) that your router should use, only the **crypto ca identity** command supports enrollment (the requesting of a router certificate from a CA). With the **crypto ca trustpoint** command, you can declare the CA and specify any characteristics for the CA that the existing commands supported.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fttrust.htm.

Tunnel Type of Service (ToS)

The Tunnel Type of Service (ToS) feature allows you to configure the ToS and Time-to-Live (TTL) byte values in the encapsulating IP header of tunnel packets for an IP tunnel interface on a router. The Tunnel ToS feature is supported on Cisco Express Forwarding (CEF), fast switching, and process switching forwarding modes.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s17/12s_tos.htm.

Unspecified Bit Rate Plus (uBR+) and ATM Enhancements for Service Provider Integrated Access

The uBR+ and ATM Enhancements for Service Provider Integrated Access feature includes:

- uBR+ functionality
- Proportional allocation of excess bandwidth
- Oversubscription of the Cisco MC3810-MFT T1/E1 trunk and similar ATM-capable VWIC-1MFT-E1 and VWIC-1MFT-T1 interface offered on the Cisco 2600 series

When uBR CPE to ATM switch is configured, a file transfer from one virtual circuit (VC) utilizes the entire trunk bandwidth when no other VCs (data or voice) are active. When other VCs become active with fixed committed information rates (CIRs), because uBR+ is not configured, the new VCs are not guaranteed their intended CIR. UBR+ resolves this by reallocating the configured CIRs to guarantee that all VCs achieve the appropriate throughput. If there is any remaining bandwidth, bursting up to that availability is still permitted. Because uBR allows for a continuous burst, bandwidth could be conserved by assigning a uBR class of service (CoS) to the VC. However, uBR has a variable bit rate (VBR) that constrains the burst period to a maximum burst size (MBS), rather than allowing a continuous burst. The uBR+ and ATM Enhancements for Service Provider Integrated Access feature does not have an MBS constraint.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_ubr.htm.

Update to the MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles

The **voice-port (MGCP profile)** command has been replaced by the **port (MGCP profile)** command. This command associates a voice port with the MGCP profile that is being configured.

The **port (MGCP profile)** command is used with the MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles feature that was released in Cisco IOS Release 12.2(4)T. Only the name of the command has been updated. The syntax and functionality have not changed.

Platforms supported are:

- Cisco CVA122 and Cisco CVA122E
- Cisco uBR925
- Cisco 2600 series
- Cisco 3660
- Cisco MC3810

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_mgupd.htm

VLAN Range

Using the VLAN Range feature, you can group VLAN subinterfaces together so that any command entered in a group applies to every subinterface within the group. This feature simplifies configurations and reduces command parsing.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/12b_rang.htm.

VoAAL2 Profile 9 Support for BLES Interoperability

This feature allows Cisco routers to provide VoAAL2 (Voice over ATM Adaption Layer 2) Profile 9 (G.711ulaw and G.711alaw with 44-byte voice payload) for interoperability with V5.2 and GR.303 Voice GW to Class 5 switches. This feature allows service providers to deliver voice services over xDSL and T1 ATM networks from Class 5 switches.

Voice Support for Japan on Cisco 800 Series Routers, Phase 2

The Enhanced Voice Services for Japan for Cisco 800 Series Routers, Phase 2 features consist of the following voice capabilities for the Cisco 800 series routers:

Intercom

This feature establishes a voice connection between the two plain old telephone service (POTS) ports within the router. No B channels are used for calling between ports, so the B channels are available for data calls. During an intercom call, call waiting is disabled. If an external call comes to either POTS port, no call waiting tone is generated. The calling party will hear a busy signal. The flash hook and dual tone multifrequency (DTMF) keys are also disabled.

An intercom call is established by pressing **0# on the handset of either POTS port. If either port is busy with an external voice call, the intercom call will not be established.

Redial

This feature allows the user on each POTS port to redial the last number dialed on that port. Redial is activated when the user presses **4# on the handset. The router will store a number of up to 65 digits for each port. Feature access codes starting with an asterisk (*), interactive voice response (IVR) digits, or the pound (#) key are not stored.

The redial feature is supported separately on each POTS port.

Local Call Transfer

An external call received on either POTS port can be transferred to the other port. The transfer is initiated by pressing the flash hook followed by **0# on the handset.

This feature does not support conference calls.

Volume Adjustments

This feature allows the adjustment of the receiver volume on each POTS port. Volume adjustment is configured using command-line interface (CLI) commands, separately for each port.

To configure the telephone receiver volume on each port, use the CLI (the **volume** command).

Distinctive Ringing Based on Caller ID

This feature allows the user to register with the router up to 20 different numbers for each POTS port and to assign distinctive ring cadences to each of these numbers. Three different cadences are available. One of the cadences is the normal ring cadence as defined by Nippon Telegraph and Telephone (NTT) and is the default cadence for unregistered numbers. Numbers are registered, and ring cadences are assigned using CLI commands.

This feature is similar to the Nariwake feature available by subscription from NTT. However, this feature does not require the user to subscribe to any special service from the service provider. If the user already subscribes to Nariwake, Nariwake takes precedence over this feature.

The ring cadences used for this feature are the same as those used by the Nariwake feature.

Distinctive ringing based on caller ID is configured using the CLI (the **caller-number** command).

Subaddresses for POTS Ports

This feature allows the router to assign ISDN subaddresses to the POTS ports. With the subaddressing properly configured on the router, an external call is able to reach the dialed destination directly.

The subaddress for each POTS port is configured separately using the CLI (the **subaddress** command).

Silent Fax Calls

This feature allows either POTS port to be configured as a Type 2 Smart Fax port. When configured in this way, the router will not generate a ring alert when a call comes into the port. Instead, a silent fax tone will be generated, to which the Type 2 Smart Fax machine will respond. The fax machine does not ring, but the fax call gets connected. If a telephone is connected instead of a fax machine, the telephone does not ring.

This feature is configured using the CLI (the **silent-fax** command).

PIAFS Support

This feature provides support for the Personal Handyphone System (PHS) Internet Access Forum Standard (PIAFS). PIAFS is a standard error correction protocol for cellular data communication that has been developed in Japan. It is designed to pass data over the PHS cellular system. It also provides transmission control procedures (comparable to OSI reference model Layer 2) for high-quality data transmission. Both PIAFS version 2.0 and version 2.1 are supported on Cisco 803, 804, and 813 routers.

The common applications that are supported using PIAFS in PHS data communications are as follows:

- E-mail—E-mail is a basic service of the PHS multimedia communications menu. This service enables the user to send and receive e-mail.
- Fax service—The data stored in a personal digital assistant (PDA) can be faxed.
- Internet access—Internet access has influenced PHS in that many users want to be able to obtain necessary information in a timely manner when they are outdoors. It is also projected that PHS will be used extensively to form intranets for in-house communications by facilitating the expansion of office LAN access points.
- Photograph transmission service—The signals of a digital still camera can be transmitted directly or through the medium of a personal computer.
- Mobile office service—The spread of groupware recently has led to frequent instances in which groups share common databases in carrying out or supporting the execution of collaborative work. Demands are being made to extend this collaborative environment even to outside locations by using mobile communications.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ktna2.htn

VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP

The VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP feature introduces support to make the following RADIUS attributes VRF aware: attribute 22 (Framed-Route), a combination of attribute 8 (Framed-IP-Address) and attribute 9 (Framed-IP-Netmask), and the Cisco VSA route command. Thus, static IP routes can be applied to a particular VRF routing table rather than the global routing table.

WRED Enhancement—Explicit Congestion Notification (ECN)

Currently, the congestion control and avoidance algorithms for TCP are based on the idea that packet loss is an appropriate indication of congestion on networks that transmit data using the best-effort service model. When a network uses the best-effort service model, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. However, these algorithms and the best-effort service model are not suited to applications that are sensitive to delay or packet loss (for instance, interactive traffic including Telnet, web browsing, and transfer of audio and video data). Weighted random early detection (WRED), and by extension, Explicit Congestion Notification (ECN), helps to solve this problem.

To indicate congestion, WRED drops packets on the basis of the average queue length exceeding a specific threshold value. ECN is an extension to WRED in that ECN marks packets instead of dropping them when the average queue length exceeds a specific threshold value. When configured with the WRED Enhancement—Support for Explicit Congestion Notification feature, routers and end hosts would use this marking as a signal that the network is congested and slow down sending packets.

This feature provides an improved method for congestion avoidance by allowing the network to mark packets for transmission later, rather than dropping them from the queue. Marking the packets for transmission later accommodates applications that are sensitive to delay or packet loss and provides improved throughput and application performance.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftwrdecn.htm.

X.25 Over TCP Profiles

The Cisco X.25 over TCP (XOT) service was originally developed as an X.25 class of service that was only designed to switch X.25 traffic across an IP network. This service allowed network administrators to connect X.25 devices across the rich connectivity and media features available to IP traffic. XOT uses a set of default parameters to make this type of network easy to design.

When the XOT' capabilities were enhanced to support packet assembler/disassembler (PAD) traffic on an XOT session, network designers saw a need to be able to configure parameters for increased flexibility. For instance, because XOT does not have any physical interfaces that an administrator can configure, PAD over XOT sessions cannot be configured with interface map or facility commands to establish a PAD connection using nondefault values.

The introduction of X.25 profiles for XOT allows the network designer added flexibility to control the X.25 class services of XOT for PAD and XOT switching usage.

Another important aspect of this feature is that it allows you to associate access lists with XOT connections, enabling you to apply security on the basis of IP addresses and to have a unique X.25 configuration for specified IP addresses.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_xotp.htm.

X.25 Record Boundary Preservation for Data Communications Networks

The X.25 Record Boundary Preservation for Data Communications Networks feature enables hosts using TCP/IP-based protocols to exchange data with devices that use the X.25 protocol, retaining the logical record boundaries indicated by use of the X.25 "more data" bit (M-bit).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdcnrbp.htm.

Hardware Platforms and Modules Newly Supported in Cisco IOS Release 12.2(4)T

The following hardware platforms and modules are now supported in Cisco IOS Release 12.2(4)T. These platforms and modules were first introduced in earlier Cisco IOS software releases.

1-Port ADSL WAN Interface Card

The 1-Port ADSL WAN Interface Card (WIC) provides ADSL high-speed digital data transfer between a single customer premises equipment (CPE) subscriber and the central office.

The ADSL WIC is compatible with the Alcatel Digital Subscriber Loop Access Multiplexer (DSLAM) and the Cisco 6130, Cisco 6160, and Cisco 6260 DSLAMs with Flexi-line cards. It supports ATM Adaptation Layer 2 (AAL2) and AAL5 for the Cisco 2600 series and Cisco 3600 series routers and AAL5 only for the Cisco 1700 series routers, for both voice and data service.

Refer to the following documents for additional information:

- Cisco 1700 series, Cisco 2600 series, and Cisco 3600 series routers:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_adsl4.htm.

- Cisco IAD2420 series platforms:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xr/121xr_5/ftiaddsl.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(2)T on the Cisco 1700 series routers. This release is porting the feature into the Cisco 2600 series and Cisco 3600 series routers and the Cisco IAD2420 series platforms.

1-Port T1/E1 Digital Voice Port Adapters for Cisco 7200 and Cisco 7500

The PA-VXB and the PA-VXC are multichannel packet voice port adapters that allow Cisco 7200 series routers, Cisco 7200 VXR routers, Cisco 7401ASR routers, and Cisco 7500 series routers to become dedicated packet voice hubs or packet voice gateways that connect to both private branch exchanges (PBXs) and the Public Switched Telephone Network (PSTN). With this technology, packet voice and packet fax calls can be placed over the WAN and sent through the gateway into the traditional circuit-switched voice infrastructure. The PA-VXB and PA-VXC are single-width port adapters with t universal ports that are configurable for either T1 or E1 connections. The PA-VXB contains 12 high-performance digital signal processors (DSPs) that support up to 48 medium-complexity or 24 high-complexity channels of compressed voice. The PA-VXC contains 30 high-performance DSPs that support up to 120 medium-complexity or 60 high-complexity channels of compressed voice.

In Voice over IP (VoIP), the DSP segments the voice signal into frames, which are then coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323. Because VoIP is a delay-sensitive application, you must have a well-engineered end-to-end network to use it successfully. Fine-tuning your network to adequately support VoIP involves a series of protocols and features geared toward quality of service (QoS). Traffic shaping considerations must be taken into account to ensure the reliability of the voice connection.

8-Port Mix-Enabled T1/E1/PRI PA

The PA-MC-8TE1+ port adapter is a single-wide port adapter that provides eight T1 or E1 interfaces for Cisco 7200 series routers. The PA-MC-8TE1+ interfaces can be channelized, fractional, or unframed (E1 only).

The PA-MC-8TE1+ provides the following features:

- Universal ports—Eight interface ports per port adapter are configurable as either T1 (with integrated channel service unit [CSU] and data service unit [DSU]) or E1 (with integrated G.703/G.704 balanced 120-ohm interface).
- Full DS0 channelization capability for all T1/E1 ports, for a maximum of 248 full-duplex HDLC channels.
- Data rates in multiples of 56 kbps or 64 kbps per channel.
- Maximum data rates per port:1.536 Mbps (T1), 1.984 Mbps (E1 G.704), 2.048 Mbps (E1 unframed).
- Integrated T1/E1 supporting linecode AMI, B8SZ (T1), framing AMI or HDB3 (E1), framing SF or ESF (T1), CRC4, no-CRC4 or unframed (E1).
- Full Facility Data Link (FDL) support and FDL performance monitoring per-ANSI T1.403 or AT&T TR 54016.
- Full ISDN support for either 23B+D (T1) or 30B+D via network processing engine (NPE).
- Performance monitoring.

- Alarm integration, detection, and insertion.
- Line and payload loopback on a per-DS0 level.
- BERT functionality to transmit and receive test patterns over any Nx64 channel group.
- Clock jitter attenuators.
- Line or internal clocking.

Refer to the *PA-MC-8TE1+ Port Adapter Installation and Configuration Note* for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/portadpt/multicha/8port_t1/index.htm.

Cisco 1751 Router

The voice-and-data capable Cisco 1751 router provides global Internet and company intranet access and includes the following:

- Voice-over-IP (VoIP) voice-and-data functionality; the router can provide support for digital and analog voice traffic (for example, telephone calls and faxes) over an IP network.
- Support for virtual private networking
- Modular architecture
- Network device integration

Cisco uBR925 Cable Access Router

The Cisco uBR925 cable access router acts as a cable modem to connect computers and other customer premises equipment (CPE) devices at a subscriber site to the service provider cable, hybrid fiber-coaxial (HFC), and IP backbone network. The Cisco uBR925 router is based on the Data-over-Cable Service Interface Specifications (DOCSIS) and interoperates with any bidirectional, DOCSIS-qualified cable modem termination system (CMTS).

The Cisco uBR925 cable access router supports both data and Voice over IP (VoIP) traffic via a shared two-way cable system and IP backbone network. PCs and other CPE devices can connect to the Cisco uBR925 router either through a four-port Ethernet hub or through the Universal Serial Bus (USB) port of the router. Single-line telephones, fax, or modems can be connected to two RJ-11 analog voice ports of the router. The Cisco uBR925 router supports DOCSIS-compliant bridging data operations, and it can also function as an advanced router, providing WAN data and VoIP connectivity in a variety of configurations.

Cisco CVA122 Cable Voice Adapter

The Cisco CVA122 Cable Voice Adapter acts as a cable modem to connect computers and other customer premises equipment (CPE) devices at a subscriber site to the service provider cable, hybrid fiber-coaxial (HFC), and IP backbone network. The Cisco CVA122 Cable Voice Adapter is based on the Data-over-Cable Service Interface Specifications (DOCSIS) and interoperates with any bidirectional, DOCSIS-qualified cable modem termination system (CMTS).

The Cisco CVA122 Cable Voice Adapter supports both data and Voice over IP (VoIP) traffic via a shared two-way cable system and IP backbone network. PCs and other CPE devices can connect to the cable voice adapter either through an Ethernet port or through a Universal Serial Bus (USB) port. Single-line telephones, fax, or modems can be connected to two RJ-11 analog voice ports of the cable voice adapter. The cable voice adapter supports DOCSIS-compliant bridging data operations, and it can also function as an advanced router, providing WAN data and VoIP connectivity in a variety of configurations.

Cisco CVA122E Cable Voice Adapter

The Cisco CVA122E Cable Voice Adapter acts as a cable modem to connect computers and other customer premises equipment (CPE) devices at a subscriber site to the service provider cable, hybrid fiber-coaxial (HFC), and IP backbone network. The Cisco CVA122E Cable Voice Adapter is based on the European Data-over-Cable Service Interface Specifications (EuroDOCSIS) and interoperates with any bidirectional, EuroDOCSIS-qualified cable modem termination system (CMTS).

The Cisco CVA122 Cable Voice Adapter supports both data and Voice over IP (VoIP) traffic via a shared two-way cable system and IP backbone network. PCs and other CPE devices can connect to the cable voice adapter either through an Ethernet port or through a Universal Serial Bus (USB) port. Single-line telephones, fax, or modems can be connected t o two RJ-11 analog voice ports of the cable voice adapter. The cable voice adapter supports EuroDOCSIS-compliant bridging data operations, and it can also function as an advanced router, providing WAN data and VoIP connectivity in a variety of configurations.

New Software Features in Cisco IOS Release 12.2(4)T

The following new features are supported in Cisco IOS Release 12.2(4)T. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

AAA-PPP-VPDN Non-Blocking

Previously, Cisco IOS created a statically configurable number of processes to authenticate calls. Each of these processes would handle a single call, but in some situations the limited number of processes could not keep up with the incoming call rate. This resulted in some calls timing out. The AAA-PPP-VPDN Non-Blocking feature changes the software architecture such that the number of processes will not limit the rate of call handling.

Ability to Disable Xauth for Static IPSec Peers

The Ability to Disable Xauth for Static IPSec Peers feature allows users to disable extended authentication (Xauth), which prevents the routers from being prompted for Xauth information—username and password.

Without the ability to disable Xauth, a user cannot select which peer on the same crypto map should use Xauth. That is, if a user has router-to-router IP Security (IPSec) on the same crypto map as a Virtual Private Network (VPN)-client-to-Cisco-IOS IPSec, both peers will be prompted for a username and password. Removing Xauth while configuring the preshared key for router-to-router IPSec, prevents duplicate Xauth information from being exchanged, thereby, reducing traffic on your network. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftnxauth.htm.

ACL Default Direction

The ACL Default Direction feature allows you to change the filter direction (where filter direction is not specified) to inbound packets only; that is, you can configure your server to filter packets that are coming toward the network.

This feature introduces the **radius-server attribute 11 direction default** command, which allows you to change the default direction of filters for your access control lists (ACL) via RADIUS. (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user.) Enabling this command allows you to change the filter direction to inbound—which stops traffic from entering a router, thereby reducing resource consumption—rather than the outbound default direction, which waits until the traffic is about to leave the network before filtering.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftacldir.htm.

Accounting of VPDN Disconnect Cause

In the past, whenever a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) session fails or disconnects, the network access server (NAS) and Home GateWay (HGW) report a very generic disconnect-cause code, such as "LOST CARRIER". These generic codes do not provide enough detailed information for accounting and debugging purposes, creating a need for disconnect-cause codes that provide more detailed information. The Accounting of VPDN Disconnect Cause feature adds eight new disconnect-cause codes. These eight disconnect-cause codes describe the status of Virtual Private Dialup Network (VPDN) failures and disconnects more specifically than existing generic disconnect-cause codes. These new disconnect-cause codes can be found in the *Cisco IOS Security Configuration Guide*, Release 12.2 located at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fappendx/fradattr/scfrdat3.htm.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftacldir.htm.

Adaptive Frame Relay Traffic Shaping for Interface Congestion

The Adaptive Frame Relay Traffic Shaping for Interface Congestion feature enhances Frame Relay traffic shaping functionality by adjusting permanent virtual circuit (PVC) sending rates based on interface congestion. When this new feature is enabled, the traffic-shaping mechanism monitors interface congestion. When the congestion level exceeds a configured value called queue depth, the sending rate of all PVCs is reduced to the minimum committed information rate (minCIR). As soon as interface congestion drops below the queue depth, the traffic-shaping mechanism changes the sending rate of the PVCs back to the committed information rate (CIR). This process guarantees the minCIR for PVCs when there is interface congestion.

This new feature works in conjunction with backward explicit congestion notification (BECN) and Foresight functionality.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_afrts.htm.

Advanced Voice Busyout

The local voice busyout feature provides a way to busy out a voice port or DS-0 group (time slot) if a state change is detected in a monitored network interface (or interfaces). When a monitored interface changes to a specified state—to out-of-service or in-service—the voice port presents a seized/busyout condition to the attached PBX or other customer premises equipment (CPE). The PBX or other CPE can then attempt to select an alternate route.

Advanced Voice Busyout adds the following functionality to the local voice busyout feature:

- For Voice over IP (VoIP), monitoring of links to remote, IP-addressable interfaces by use of service assurance agent (SAA)
- Configuration by voice class to simplify and speed up the configuration of voice busyout on multiple voice ports

Using the Advanced Voice Busyout feature you can perform the following tasks:

- Configure individual voice ports to enter the busyout state if an SAA probe signal returned from a remote, IP-addressable interface detects loss of IP connectivity by crossing a specified delay or loss threshold.
- Define voice classes with specified busyout conditions, and assign a particular voice class to any number of voice ports.
- SAA probe monitoring of remote interfaces is intended for use with VoIP networks, although it can also be used with Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_cacbo.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(3)T. This release is porting the feature into the Cisco 7200 series routers, and adds support for new and modified commands.

Asynchronous Line Monitoring

Before Cisco IOS Release 12.2(4)T, the Cisco IOS software did not provide a method for displaying asynchronous character mode traffic flowing out of an asynchronous line. Therefore, when a user tried to troubleshoot difficult asynchronous problems, the user had to use RS-232 datascopes in order to examine the data stream. This method is very detailed and cumbersome. The Asynchronous Line Monitoring feature available in Cisco IOS Release 12.2(4)T allows the monitoring of inbound and outbound character mode asynchronous traffic on another terminal line. To monitor inbound or outbound asynchronous character mode traffic on the port to be monitored, enter the **monitor traffic line** command in privileged EXEC mode.

This feature increases the efficiency of the user who performs troubleshooting on asynchronous character mode traffic problems. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftasync.htm.

ATM SNMP Trap and OAM Enhancements

The ATM SNMP Trap and OAM Enhancements feature introduces the following enhancements to the Simple Network Management Protocol (SNMP) notifications for ATM permanent virtual circuits (PVCs) and to operation, administration, and maintenance (OAM) functionality:

- ATM PVC traps will now be generated when the operational state of a PVC changes from the DOWN to UP state.
- ATM PVC traps will now be generated when OAM loopback fails. Additionally, when OAM loopback fails, the PVC will now remain in the UP state, rather than going DOWN.
- The ATM PVC traps are now extended to include virtual path interface/virtual circuit interface (VPI/VCI) information, the number of state transitions a PVC goes through in an interval, and the timestamp of the first and the last PVC state transition.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftpvctrp.htm.

AutoInstall over Frame Relay-ATM Interworking Connections

The AutoInstall over Frame Relay-ATM Interworking Connections feature extends the functionality of the existing Cisco IOS AutoInstall feature. After you connect a new router to the network and turn on the new router, Cisco IOS AutoInstall automatically configures the router from a preexisting configuration file that is downloaded from the network. This process was designed to facilitate the centralized management of router installation.

The AutoInstall over Frame Relay-ATM Interworking Connections feature allows you to configure an ATM permanent virtual circuit (PVC) to accept the BOOTP and TFTP requests from a new router performing AutoInstall. This feature also allows the use of a central router with ATM or Frame Relay IETF encapsulation to run a BOOTP server and provide an initial IP address to the new router.

For details, refer to the "AutoInstall over Frame Relay-ATM Interworking Connections" feature module document. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftautatm.htm.

Automatic Bandwidth Adjustment for MPLS Traffic Engineering Tunnels

Traffic engineering automatic bandwidth adjustment provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels based on their measured traffic load.

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, it periodically (for example, once per day) adjusts the tunnel's allocated bandwidth to be the largest sample for the tunnel since the last adjustment.

The frequency with which tunnel bandwidth is adjusted and the allowable range of adjustments is configurable on a per-tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate is user-configurable on a per-tunnel basis.

There are three new commands:

- **clear mpls traffic-eng auto-bw timers**: Reinitializes the automatic bandwidth feature.
- **mpls traffic-eng auto-bw timers**: Enables automatic bandwidth adjustment for a platform and starts output rate sampling for tunnels configured for automatic bandwidth adjustment.
- **tunnel mpls traffic-eng auto-bw**: Configures a tunnel for automatic bandwidth adjustment and controls the manner in which the bandwidth for a tunnel is adjusted.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftbwadjm.htm.

BGP Conditional Route Injection

Cisco IOS software provides several methods in which you can originate a prefix into the Border Gateway Protocol (BGP). The existing methods include using the network or **aggregate-address** commands and redistribution. These methods assume the existence of more specific routing information (matching the route to be originated) in either the routing table or the BGP table.

The BGP Conditional Route Injection feature enables you to originate a prefix into BGP without the corresponding match. The routes are injected into the BGP table only if certain conditions are met. The most common condition is the existence of a less-specific prefix.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftbgpri.htm.

BGP Link Bandwidth

The Border Gateway Protocol (BGP) Link Bandwidth feature is used to advertise the bandwidth of an autonomous system exit link as an extended community. The BGP Link Bandwidth feature is supported by the internal BGP (iBGP) and external BGP (eBGP) multipath features. The link bandwidth extended community indicates the preference of an autonomous system exit link in terms of bandwidth. The link bandwidth extended community attribute may be propagated to all iBGP peers and used with the BGP multipath features to configure unequal cost load balancing. When a router receives a route from a directly connected external neighbor and advertises this route to iBGP neighbors, the router may advertise the bandwidth of that link.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftbgplb.htm.

BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN

The BGP Multipath Load Sharing for eBGP and iBGP feature allows you to configure multipath load balancing with both external BGP (eBGP) and internal BGP (iBGP) paths in Border Gateway Protocol (BGP) networks that are configured to use Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). This feature provides improved load balancing deployment and service offering capabilities and is useful for multi-homed autonomous systems and Provider Edge (PE) routers that import both eBGP and iBGP paths from multihomed and stub networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/fteibmpl.htm.

BGP Prefix-Based Outbound Route Filtering

The BGP Prefix-Based Outbound Route Filtering feature uses Border Gateway Protocol (BGP) outbound route filter (ORF) send and receive capabilities to minimize the number of BGP updates that are sent between peer routers. The configuration of this feature can help reduce the amount of resources required for generating and processing routing updates by filtering out unwanted routing updates at the source.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftbgporf.htm.

Call Admission Control for H.323 VoIP Gateways

Call Admission Control, Call Treatment, and Busyout Components

Before the call admission control feature, gateways did not have a mechanism to gracefully prevent calls from entering when certain resources were not available to process the call. This causes the new call to fail with unreported behavior, and could potentially cause the calls that are in progress to have quality related problems.

This feature set provides the ability to support resource-based call admission control processes. These resources include system resources such as CPU, memory, and call volume, and interface resources such as call volume.

If system resources are not available to admit the call, two kinds of actions are provided: system denial (which busyouts all of T1 or E1) or per call denial (which disconnects, hairpins, or plays a message or tone). If the interface-based resource is not available to admit the call, the call is dropped from the session protocol (such as H.323).

For further information on busyout, please refer to *Advanced Voicebusyout*, Cisco IOS Release 12.2(2)XA. For further information on the call denial aspects of this feature, please refer to *Call Admission Control Based on CPU Utilization*.

User Selected Threshold

This feature allows a user to configure call admission thresholds for local resources as well as memory and CPU resources. The list of local resources that are configured for call admission are described in the command description of "call threshold poll-interval."

With the **call threshold** command, a user is allowed to configure two thresholds, high and low, for each resource. Call treatment is triggered when the current value of a resource goes beyond the configured high. The call treatment remains in effect until current resource value falls below the configured low. Having high and low thresholds prevents call admission flapping and provides hysteresis in call admission decision making.

With the **call spike** command, a user is allowed to configure the limit for incoming calls during a specified time period. A call spike is the term for when a large number of incoming calls arrive from the PSTN in a very short period of time (for example: 100 incoming calls in 10 milliseconds).

Configurable Call Treatment

With the **call treatment** command, users are allowed to select how the call should be treated when local resources are not available to handle the call. For example, when the current resource value for any one of the configured triggers for call threshold has reached beyond the configured threshold, the call treatment choices are as follows:

- Time- division multiplexing (TDM) hairpinning — Hairpins the calls through the plain old telephone service (POTS) dial peer.
- Reject — Disconnects the call.
- Play message or tone — Plays a configured message or tone to the user.

Resource Unavailable Signaling

This feature set supports the autobusyout feature where channels are busied out when local resources are not available to handle the call. Autobusyout is supported on both channel-associated signaling (CAS) and PRI channels.

- CAS — Uses busyout to signal "local resources are unavailable."
- PRI — Uses either service messages or disconnect with correct cause-code to signal "resources are unavailable."

PSTN Fallback

The goal of PSTN fallback is to monitor congestion in the IP network and either redirect calls to the PSTN or reject calls based on the network congestion. Calls can be rerouted to an alternate IP destination or to the PSTN if the IP network is found unsuitable for voice traffic at that time. The user defines the congestion thresholds based on the configured network. This functionality enables the service provider to give a reasonable guarantee about the quality of the conversation to their VoIP users at the time of call admission.

Note PSTN fallback does not provide assurances that a VoIP call that proceeds over the IP network is protected from the effects of congestion. This is the function of the other Quality of Service (QoS) mechanisms such as IP Real-Time Transport Protocol (RTP) priority or low latency queuing (LLQ).

PSTN fallback includes the following features:

- Offers flexibility to define the congestion thresholds based on the network.
  - Defines a threshold based on Calculated Planning Impairment Factor (ICPIF), which is derived as part of International Telecommunication Union (ITU) G.113.
  - Defines a threshold based solely on packet delay and loss measurements.
- Uses Service Assurance Agent (SAA) probes to provide packet delay, jitter, and loss information for the relevant IP addresses. Based on the packet loss, delay, and jitter encountered by these probes, an ICPIF or delay and loss values are calculated.
- Is supported by calls of any codec. Only G.729 and G.711 have accurately simulated probes. Calls of all other codecs are emulated by a G.711 probe.

For more information, including configuration tasks and examples, and command references for PSTN fallback, please refer to PSTN Fallback. Refer to the following document for additional information about the Call Admission Control for H.323 VoIP Gateways feature:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_pfavb.htm.

Circuit Interface Identification Persistence for SNMP

The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object (cciDescr) which can be used to identify individual circuit-based interfaces for SNMP monitoring. The Circuit Interface Identification Persistence for SNMP feature maintains this user-defined name of the circuit across reboots, allowing the consistent identification of circuit interfaces. Circuit Interface Identification Persistence is enabled using the **snmp mib persist circuit** global configuration command.

Cisco H.323 Scalability and Interoperability Enhancements

The Cisco H.323 Scalability and Interoperability Enhancements feature upgrades the Cisco H.323 Gatekeeper and Cisco H.323 Gateway to comply with H.323 Version 3. The enhancements in this release include support for mandatory H.323 Version 3 elements in the gateway, support for H.225 call signalling over User Datagram Protocol (UDP), and address resolution using border elements.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/fth323v3.htm.

Cisco Mobile Networks

The Cisco Mobile Networks feature enables a Mobile Router and its subnets to be mobile and maintain all IP connectivity, transparent to the IP hosts connecting through this Mobile Router.

Mobile IP, as defined in standard RFC 2002, provides the architecture that enables the Mobile Router to connect back to its home network. Mobile IP allows devices to roam while appearing to be at their home network. Such a device is called a mobile node. A mobile node is a node, for example, a personal digital assistant, a laptop computer, or a data-ready cellular phone, that can change its point of attachment from one network or subnet to another. This mobile node can travel from link to link and maintain ongoing communications while using the same IP address.

The Mobile Router functions similarly to the mobile node with one key difference—the Mobile Router allows entire networks to roam. For example, a plane with a Mobile Router can fly around the world while passengers stay connected to the Internet. This communication is accomplished by Mobile IP aware routers tunneling packets, which are destined to hosts on the mobile networks, to the location where the Mobile Router is visiting. The Mobile Router then forwards the packets to the destination device.

These devices can be mobile nodes running mobile IP client software or nodes without the software. The Mobile Router eliminates the need for a mobile IP client. In fact, the nodes on the mobile network are not aware of any IP mobility at all. The Mobile Router "hides" the IP roaming from the local IP nodes so that the local nodes appear to be directly attached to the home network.

The Cisco Mobile Networks feature is a static network implementation that supports stub routers only. The Mobile Router avoids convergence problems by statically defining which networks it can address. The Mobile Router can do the following:

- Perform agent solicitation
- Perform registration and reregistration
- Decapsulate information for its attached devices

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.htm.

Cisco Modem User Interface

The Cisco Modem User Interface feature enables Cisco routers to behave like a modem and be configured using standard Hayes modem commands. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftcmodui.htm.

Configuring AAL2 and AAL5 for the High Performance ATM Advanced Integration Module on the Cisco 2600 Series

The High Performance ATM Advanced Integration Module (AIM) is an internally mounted card that offers a cost-effective solution for supporting low-speed ATM WAN connections on the Cisco 2600 family of products. When using the voice DSP capability of a digital T1/E1 packet voice trunk network module (NM-HDV) and a T1/E1 multiflex VWIC, it supports as many as 60 channels of compressed voice over a T1/E1 trunk using AAL2 or AAL5, without using a dedicated ATM network module. AAL2 and AAL5 are the most bandwidth-efficient standards-based trunking methods for transporting compressed voice, voice-band data, circuit-mode data, and frame-mode data over ATM infrastructures. This feature provides a cost-effective, low-density ATM T1 or E1 solution for the Cisco 2600 series.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_24aim.htm.

CNS Configuration Agent

CNS is a foundation technology for linking users to network services. CNS SDK accomplishes this by making applications network-aware and increasing the intelligence of the network elements. CNS SDK provides building blocks to a range of customers in market segments such as Enterprise, service provider, independent software vendors, and system integrators.

The CNS Configuration Agent supports routing devices by providing:

- Initial configurations
- Incremental (partial) configurations
- Synchronized configuration updates

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcns_ca.htm.

CNS Event Agent

CNS is a foundation technology for linking users to network services. CNS SDK accomplishes this by making applications network-aware and increasing the intelligence of the network elements. CNS SDK provides building blocks to a range of customers in market segments such as Enterprise, service provider, independent software vendors, and system integrators.

The CNS Event Agent is part of the Cisco IOS infrastructure that allows Cisco IOS applications, for example CNS Configuration Agent, to publish and subscribe to events on a CNS Event Bus. CNS Event Agent works in conjunction with CNS Configuration Agent.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcns_ea.htm.

Crashinfo Support for Cisco 3600 Series

Crashinfo is a mechanism to reliably and quickly store useful information related to unexpected system shutdowns directly to a local flash card. This information can be retrieved after a system reload to aid in the analysis and resolution of a system error.

Cisco IOS Release 12.2(4)T introduces crashinfo support for the Cisco 3600 series. To enable this feature, use the **exception crashinfo file** *device:filename* in global configuration mode. Use the device and filename arguments to specify the flashcard and file to be used for storing the diagnostic information. To change the size of the crashinfo buffer, use the **exception crashinfo buffersize** command. The default buffer size is 32 Kilobytes.

DFP Support in DistributedDirector

DistributedDirector can obtain load information from Cisco LocalDirector, Catalyst 4840g, and other clients using Dynamic Feedback Protocol (DFP). This protocol allows the user to configure the DistributedDirector to communicate with various DFP agents. The DistributedDirector tells the DFP agents how often they should report load information; then the DFP agent can tell the DistributedDirector which LocalDirector cluster to remove from providing service.

Dialer CEF

The Dialer CEF feature introduces Cisco Express Forwarding (CEF) support for dialer interfaces. The Dialer CEF feature allows packets to be CEF switched across dialer interfaces rather than being low-end switched (LES) or fast switched. Compared to fast switching, CEF switching support improves switching performance by decreasing CPU utilization and lowering the packet loss rate. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftdlrcef.htm.

Dialer Persistent

The Dialer Persistent feature allows the connection settings in a dial-on-demand routing (DDR) dialer profile to be configured as *persistent*, that is, the connection is not torn down until the **shutdown** EXEC command is entered on the dialer interface. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftdperst.htm.

Diff-Serv-aware Traffic Engineering

MPLS traffic engineering allows constraint-based routing of constant bit rate (CBR) IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. Diff-Serv-aware Traffic Engineering extends MPLS traffic engineering to enable you to perform constraint-based routing of "guaranteed" traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher Quality of Service performance (in terms of delay, jitter, or loss) for the guaranteed traffic.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_ds_te.htm.

Distinguished Name Based Crypto Maps

The Distinguished Name Based Crypto Maps feature allows you to restrict access to selected encrypted interfaces to peers with specific certificates, especially certificates with particular Distinguished Names (DNs).

Initially, if the router accepted a certificate or a shared secret from the encrypting peer, Cisco IOS did not have a method of preventing the peer from communicating with any encrypted interface other than the restrictions on the IP address of the encrypting peer. This feature allows you to configure which crypto maps are usable to a peer based on the DN that a peer used to authenticate itself. Thus, enabling you to control which encrypted interfaces a peer with a specified DN can access.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftdnacl.htm.

Distributed Link Fragmentation and Interleaving

The Distributed Link Fragmentation and Interleaving feature extends Link Fragmentation and Interleaving functionality to VIP-enabled Cisco 7500 series routers.

The Distributed Link Fragmentation and Interleaving feature supports the transport of real-time traffic, such as voice, and non real-time traffic, such as data, on lower-speed Frame Relay and ATM virtual circuits (VCs) without causing excessive delay to the real-time traffic.

This feature implements link fragmentation and interleaving (LFI) using multilink PPP (MLP) over Frame Relay and ATM. The feature enables delay-sensitive real-time packets and packets that are not real-time data to share the same link by fragmenting the large data packets into a sequence of smaller data packets (fragments). The fragments are then interleaved with the real-time packets. On the receiving side of the link, the fragments are reassembled and the packet is reconstructed.

Distributed LFI is often useful in networks that send real-time traffic, such as voice, but have bandwidth problems that delay this real-time traffic due to the transport of large, less time-sensitive data packets. Distributed LFI can be used in these networks to disassemble the large data packet into multiple segments. The real-time traffic packets can then be sent between these segments of the data packet. In this scenario, the real-time traffic does not experience a lengthy delay waiting for the low-priority data packet to traverse the network. The data packet is reassembled at the receiving side of the link, so the data is delivered intact.

DistributedDirector Enhancements

This release of Cisco DistributedDirector contains two new commands. The new **ip director default priorities** command specifies the default priorities for each type of metric. If a metric does not have a default priority specified, DistributedDirector does not use that metric. The default priorities take effect if no priorities are specified in the DNS TXT record for that host.

The new **ip director drp rttprobe tcp | icmp** command enables DistributedDirector to instruct a DRP agent to send ICMP-echo packets to measure the RTT.

The new **show ip director default priority** command verifies the default priority configurations.

The **ip director default-weights** command has been modified. It is now **ip director default weights**.

The **show ip director default-weights** command has been modified. It is now **show ip director default weights**.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftdd1224.htm.

Distributed Management Event and Expression MIB Persistence

The MIB Persistence feature allows the SNMP data of an MIB to be persistent across reloads; that is, MIB information retains the same set object values each time the user reboots. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmibpr1.htm.

DNS Server Support for NS Records

DistributedDirector has improved server load-balancing capacity with the DNS Server Support for NS Records feature. This feature adds support for name server (NS) records to the Cisco IOS Domain Name System (DNS) server. With this feature, the DistributedDirector can distribute the server-selection process to multiple DistributedDirectors, improving overall server capacity.

Enhanced Test Command

The Enhanced Test Command feature introduces two new commands—**aaa user profile** and **aaa attribute**—that allow you to create a named user profile with calling line identification (CLID) or dialed number identification service (DNIS) attribute values, which can be associated with a **test aaa group** command.

Use the **aaa attribute** command to add CLID or DNIS attribute values to a user profile, which is created by using the aaa user profile command. The CLID or DNIS attribute values can be associated with the record that is going out with the user profile (via the test aaa group command), thereby providing the RADIUS server with access to CLID or DNIS attribute information for all incoming calls.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftaaacmd.htm.

Enhancements to H.323 Call Statistics

Beginning with Cisco IOS Release 12.2(4)T, enhancements to H.323 call statistics allow you to clear the gateway counters, display H.323 messages that have been sent and received, obtain statistics on the reasons calls are disconnected, and display debug output for various components within the H.323 subsystem. To enable these enhancements, the following commands have been added or modified: **clear h323 gateway**, **show h323 gateway**, and **debug cch323**.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftcallst.htm.

Firewall Authentication Proxy

The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. Previously, user identity and related authorized access was associated with the IP address of a user, or a single security policy had to be applied to an entire user group or sub network. Now, users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, as opposed to general policy applied across multiple users.

With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS, or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with other Cisco IOS security features such as Network Address Translation (NAT), Context-based Access Control (CBAC), IP Security (IPSec) encryption, and Cisco Secure VPN Client (VPN client) software.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scprt3/scdauthp.htm.

Four SS7 Link Support on the Cisco Signaling Link Terminal

The Four SS7 Link Support on the Cisco Signaling Link Terminal feature introduces support for up to four Cisco SS7 links on a new platform for the Cisco SLT, the Cisco 2651 Multiservice Access Router. All existing Cisco 2611-based Cisco SLT functionality is supported on the new platform, and both Cisco SLT platforms use the same Cisco IOS software image.

The Cisco 2651-based Cisco SLT supports up to four SS7 A-links and F-links, and each SS7 link can support up to 0.4 erlangs of signaling traffic during normal operation. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_4lnk.htm.

Frame Relay 64-Bit Counters

The Frame Relay 64-Bit Counters feature provides 64-bit counter support on Frame Relay interfaces and subinterfaces. This feature enables the gathering of statistics through Simple Network Management Protocol (SNMP) for faster interfaces operating at OC-3, OC-12, and OC-48 speeds.

The following counters are supported by this feature: Bytes In, Bytes Out, Packets In, and Packets Out.

The **show frame-relay pvc** command has been modified to display the 64-bit counters. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft64bits.htm.

Frame Relay MIB Enhancements

The Cisco Frame Relay MIB describes managed objects that enable users to remotely monitor Frame Relay operations using Simple Network Management Protocol (SNMP). The Frame Relay MIB Enhancements feature extends the Cisco Frame Relay MIB by adding MIB objects to monitor the following Frame Relay functionality:

- Frame Relay fragmentation
- Frame Relay–ATM Network Interworking (FRF.5)
- Frame Relay–ATM Service Interworking (FRF.8)
- Frame Relay switching
- Input and output rates of individual virtual circuits (VCs)

The Frame Relay MIB enhancements also modify the **load-interval** command to enable you to configure the load interval per permanent virtual circuit (PVC). Before the introduction of this feature, the load interval could be configured only for the interface. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftfrmibe.htm.

High-Performance Gatekeeper

The Cisco High-Performance Gatekeeper feature introduces new gatekeeper functionality and modifications for facilitating carrier class reliability, security, and performance into the Cisco Voice Network solution portfolio. These H.323 standard-based features have carrier grade reliability and performance characteristics with a robust open application protocol interface to enable development of enhanced applications like voice Virtual Private Networks (VPNs) and wholesale voice solutions.

This feature addresses the scalability, redundancy, and performance aspects of the gatekeeper as part of the Cisco Multimedia Conference Manager (MCM) to present a complete Cisco solution. The Cisco H.323 MCM provides the network administrator with the ability to identify H.323 traffic and to apply appropriate policies.

iBGP Multipath Load Sharing

When a Border Gateway Protocol (BGP) speaker router with no local policy configured receives multiple network layer reachability information (NLRI) from the internal BGP for the same destination, the router will choose one internal BGP path as the best path. The best path is then installed in the IP routing table of the router.

The Internal BGP Multipath Load Sharing feature enables the BGP speaker router to select multiple internal BGP paths as the best paths to a destination. The best paths or multipaths are then installed in the IP routing table of the router.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11bmls.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco 1710, Cisco 1721, Cisco 1751, Cisco 3631, Cisco 3725, and Cisco 3745 routers, and the IGX 8400 series URM.

ICMP ECHO-Based RTT Probing by DRP Agents

DistributedDirector users can now control Director Response Protocol (DRP) agents to send both TCP and ICMP packets for round-trip time (RTT) measurement.The RTT measurement is used to dynamically direct Internet customers to the closest regional web proxy based on response time.

In the original implementation, some Internet DNS servers did not respond when the DRP agents sent them a query to measure the RTT.

This feature introduces the new **ip director drp rttprobe tcp** | **icmp** command that enables DistributedDirector to instruct a DRP agent to send ICMP-echo packets to measure the RTT.

When both ICMP and TCP are enabled, DistributedDirector will instruct DRP agents to send both TCP and ICMP packets for RTT probing. The returned RTT from a DRP agent will be the RTT collected from either the TCP or ICMP mechanism, which ever becomes available first.

IGMP MIB Support Enhancements for SNMP

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to neighboring multicast routers. The IGMP MIB describes objects that enable users to remotely monitor and configure IGMP using Simple Network Management Protocol (SNMP). It also allows users to remotely subscribe and unsubscribe from multicast groups. The IGMP MIB Support Enhancements for SNMP feature adds full support of RFC 2933 (Internet Group Management Protocol MIB) in Cisco IOS software. There are no new or modified Cisco IOS commands associated with this feature.

For complete details on the IGMP MIB, see the IGMP-STD-MIB.my file available from the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Inter-Domain Gatekeeper Security Enhancement

The Inter-Domain Gatekeeper Security Enhancement provides a means of authenticating and authorizing H.323 calls between the administrative domains of Internet Telephone Service Providers (ITSPs).

An interzone ClearToken (IZCT) is generated in the originating gatekeeper when a location request (LRQ) is initiated or an admission confirmation (ACF) is about to be sent for an intrazone call within an ITSP administrative domain. As the IZCT traverses through the routing path, each gatekeeper stamps the IZCT destination gatekeeper ID with its own ID. This identifies when the IZCT is being passed over to another ITSP domain. The IZCT is then sent back to the originating gateway in the location confirmation (LCF) message. The originating gateway passes the IZCT to the terminating gateway in the SETUP message. The terminating gatekeeper forwards the IZCT in the admission request (ARQ) answerCall field to the terminating gatekeeper, which then validates it.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_ctoke.htm.

Interesting Traffic PPP and Customer Profile Idle Timer

The Interesting Traffic PPP and Customer Profile Idle Timer feature supports a PPP idle timer based on interesting traffic for dialer interfaces.

Interface Index Display

The Interface Index (IfIndex) is a user-specified identification number for an interface used in SNMP network management. The IfIndex is an object in the Interfaces Group MIB (IF-MIB), which can be set by a network manager to consistently identify an interface. A new Cisco IOS software command, **show snmp mib ifmib ifindex**, allows the user to display the IfIndex identification numbers assigned to interfaces and subinterfaces using the CLI. The IFIndex provides a way to display these values without the need for a Network Management Station.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftshowif.htm.

IP to ATM Class of Service Mapping for SVC Bundles

The IP to ATM Class of Service Mapping for SVC Bundles feature supports multiple switched virtual circuits (SVCs) to the same NSAP destination for different types of service (ToS). This feature is an extension to the feature described in the chapter "Configuring IP to ATM Class of Service" in the *Cisco IOS Quality of Service Solutions Configuration Guide*. The original feature was limited to permanent virtual circuits (PVCs) only. This feature is an extension because it applies to SVCs.

The PVC bundle feature requires that the user configure PVCs for different IP ToS. The PVCs have to be set up throughout the ATM network between endpoints. The IP to ATM Class of Service Mapping for SVC Bundles feature needs configuration only at the endpoints. The user does not configure SVCs; the software sets up SVCs in a bundle between endpoints. When the router receives the first IP packet for the destination that is configured in the SVC bundle, that event triggers the creation of the SVC.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftsvbund.htm.

IPSec MIB Support for VPN Management

The IPSec MIB Support for VPN Management feature allows the monitoring of IP Security (IPSec) and Internet Key Exchange (IKE) protocols using SNMP. IPSec and IKE monitoring is especially useful in Virtual Private Networks (VPNs) supporting gateway devices and customer premises equipment (CPE).

For IPSec MIB implementation details, see the CISCO-IPSEC-MIB.my, CISCO-IPSEC-POLICY-MAP-MIB.my, and CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available through the Cisco.com MIB site.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e4/dtipmib.htm.

IPv6 for Cisco IOS Software

IPv6, formerly called IPng (next generation), is a replacement for the current version of IP (version 4). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/index.htm.

IRR Triggers for GKTMP

The IRR Triggers for GKTMP feature allows a Cisco Gateway to send an information request response (IRR) to the Gatekeeper (GK) containing the details of a particular call after a successful connect. The feature also allows a back end application to set triggers for this message and the GK to deliver the IRR information to the application.

ISIS: Allows BGP to Control the Configuration of the Overload Bit

The Intermediate-System to Intermediate-System (IS-IS) protocol defines a special bit in each link-state packet (LSP) called the overload-bit. IS-IS uses the overload bit to "tell" other routers to ignore this router in their shortest path first (SPF) calculations. This function prevents transit traffic from passing through the router before the routing table has converged, and transit traffic is not lost.

L2TP IPSec

The L2TP IPSec feature provides enhanced security for tunneled PPP frames between the L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS). Previous releases of the Cisco IOS provided only a one time, optional mutual authentication during tunnel setup with no authentication of subsequent data packets or control messages. In situations where L2TP is used to tunnel PPP sessions over an untrusted infrastructure such as the internet, the security attributes of L2TP and PPP are inadequate. PPP provides no protection of the L2TP tunnel, and current PPP encryption protocols provide inadequate key management and no authentication or integrity mechanisms. The L2TP IPSec feature allows the robust security features of IPSec to protect the L2TP tunnel and the PPP sessions within the tunnel. In addition, the L2TP IPSec feature provides built in keepalives and standardized interfaces for user authentication and accounting to AAA servers.

The deployment of Windows 2000 demands the integration of IPSec with L2TP as this is the default Virtual Private Dialup Network (VPDN) networking scenario. This integration of protocols is also used for LAN-to-LAN VPDN connections in Windows 2000. The L2TP IPSec feature provides integration of IPSec with L2TP in a solution that is scalable to large networks with minimal configuration.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftl2tsec.htm.

L2TP Large-Scale Dial-Out

The L2TP Large-Scale Dial-Out feature enables the router to dial multiple Layer 2 Tunnel Protocol (L2TP) access concentrators (LACs) from a single L2TP network server (LNS). The LACs are signaled through the LNS and use L2TP to establish the dial sessions. User-defined profiles can be configured on an authentication, authorization, and accounting (AAA) server and retrieved by the LNS when dial-out occurs.The L2TP Large-Scale Dial-Out feature also supports multiple LACs bound into one stack group, call traffic load balancing, and outbound call congestion management.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftl2lsdo.htm.

Leased and Switched BRI Interfaces for ETSI NET3

The Leased and Switched BRI Interfaces for ETSI NET3 feature allows one BRI B channel on an ETSI NET3 switch to be configured as a leased line, and the second B channel to be configured as a standard ISDN or dial interface and used as a switched channel to the Public Switched Telephone Network (PSTN). When the Leased and Switched BRI Interfaces for ETSI NET3 feature is configured, one B channel functions as a point-to-point 64 kbps leased line and the other B channel functions as a circuit-switched channel using the D channel to provide the signaling features available for the ETSI NET3 signaling protocol.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftlswbri.htm.

Location Confirmation Enhancements for Alternate Endpoints

The Location Confirmation (LCF) Enhancements for Alternate Endpoints feature allows a Cisco IOS Gatekeeper (GK) to collect additional routes to endpoints that are indicated by multiple LCF responses from remote GKs, and convey a collection of those routes to the requesting (calling) endpoint. Currently, the originating GK sends Location Request (LRQ) messages to multiple remote zones. Remote GKs in the zones return LCF responses to the originating GK. The LCF responses indicate alternate routes to the remote GK endpoints.

The LCF Enhancements for Alternate Endpoints feature allows the originating GK to discover and relay more possible terminating endpoints to the requesting endpoint, therefore providing alternate routes to endpoints that can be used if the best route is busy or does not provide any alternate routes. The endpoint receiving the list of alternate endpoints tries to reach them in the order in which the alternate endpoints were received. The LCF Enhancements for Alternate Endpoints feature can be used on GKs that originate LRQs and directory GKs that forward LRQ messages.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_lcfep.htm.

Low Latency Queueing

Low Latency Queueing is now supported on Cisco 820 routers. The Low Latency Queueing feature brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority queueing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic. Information about LLQ is provided in the *Quality of Service Solutions Configuration Guide*. For overview information, refer to the following chapter:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt2/qcfconmg.htm#xtocid1239530.

For configuration instructions, refer to the following chapter:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt2/qcfwfq.htm#xtocid2836441.

MD5 File Validation

The MD5 File Validation feature allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

To perform the MD5 integrity check, execute the verify command using the new "/md5" keyword. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /md5** command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /MD5 8b5f3062c4caeccae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch.

A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles

This feature implements the following MGCP protocols on Cisco media gateways:

- MGCP 1.0 (IETF RFC2705), which applies to both trunking gateways and residential gateways.
- Network-based Call Signaling (NCS) 1.0, the PacketCable profile of MGCP 1.0 for residential gateways (RGWs)
- Trunking Gateway Control Protocol (TGCP) 1.0, the PacketCable profile of MGCP 1.0 for trunking gateways (TGWs)

The MGCP 1.0 specification and the NCS and TGCP profiles support new packages, endpoints, and event definitions. In addition, the specifications provide more detail regarding error recovery. In general, the latest edition of the MGCP specification provides guidelines for more reliable implementations of the protocol.

Media Gateway Control Protocol (MGCP) 1.0 is a protocol for the control of Voice over IP (VoIP) calls by external call-control elements known as media gateway controllers (MGCs) or call agents (CAs). It is described in the informational RFC2705, published by the Internet Engineering Task Force (IETF). MGCP 1.0 provides interoperability with a wide variety of call agents, thus enabling an extensive range of solutions.

The NCS and TGCP protocol specifications were developed through PacketCable, an industry-wide initiative to develop interoperability standards for multimedia services over cable facilities using packet technology that is led by CableLabs, an industry consortium. In Europe, the EuroPacketCable working group is ensuring that packet cable standards are available to meet European requirements and equipment characteristics.

NCS and TGCP protocol specifications contain extensions and modifications to MGCP while preserving basic MGCP architecture and constructs. NCS 1.0 is designed for use with analog, single-line user equipment on residential gateways, while TGCP 1.0 is intended for use in VoIP-to-PSTN trunking gateways in a cable environment. TGCP and NCS allow participation in packet cable solutions, but the specifications do not preclude their use in non-cable environments.

Media gateway platforms supported for this feature include:

- MGCP 1.0
  - Cisco 2600 series
  - Cisco 2650
  - Cisco MC3810
- MGCP 1.0 and NCS 1.0
  - Cisco CVA122
  - Cisco CVA122E
  - Cisco uBR925
- MGCP 1.0 and TGCP 1.0
  - Cisco 3660

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_lcfep.htm.

MGCP Voice Gateway Interoperability with Cisco CallManager

MGCP voice gateway interoperability with Cisco CallManager allows modular access routers to act as redundant failover MGCP gateways. You can enable IP telephony and Cisco CallManager solutions using Cisco 2600 and Cisco 3600 series routers as voice gateways. This allows you to use the Cisco 2600 and 3600 platforms already in your networks as MGCP gateways within an IP telephony architecture.

An MGCP gateway handles the translation between audio signals and the packet network. The gateways interact with a call agent (also called a Media Gateway Controller or MGC) that performs signal and call processing on gateway calls.

In the MGCP configurations that Cisco IOS supports, the gateway can be any of the following:

- Cisco router
- Access server
- Cable modem

The call agent is either of the following:

- A server from a third-party vendor
- Cisco CallManager

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_mgccm.htm.

Mobile IP MIB Support for SNMP

The Mobile IP MIB Support for SNMP feature adds a MIB module which expands network monitoring capabilities of Foreign Agent (FA) and Home Agent (HA) Mobile IP Entities. Mobile IP management using SNMP is defined in two MIBs: the RFC2006-MIB and the CISCO-MOBILE-IP-MIB. The Cisco Mobile IP MIB is a Cisco enterprise-specific extension to IETF RFC 2006 MIB module which allows you to monitor the total number of HA Mobile bindings and the total number of FA visitor bindings. This release also adds support for RFC 2006 Set operations and a SNMP notification. Set operations (performed from a Network Management System) are supported for starting and stopping the mobile IP service, configuring security associations, modifying advertisement parameters, and configuring "care-of addresses" for foreign agents. An SNMP notification (trap or inform) for security violations can be enabled on supported routing devices using the **snmp-server enable traps ipmobile** and **snmp-server host** global configuration CLI commands. As this feature affects security, use of SNMPv3 is strongly recommended.

For further details, refer to the *Mobile IP MIB Support for SNMP* Feature Guide at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t1/ft1mip.htm.

Mobile Networks

The Cisco Mobile Networks feature enables a Mobile Router and its subnets to be mobile and maintain all IP connectivity, transparent to the IP hosts connecting through this Mobile Router.

Mobile IP, as defined in standard RFC 2002, provides the architecture that enables the Mobile Router to connect back to its home network. Mobile IP allows a device to roam while appearing to be at its home network. Such a device is called a mobile node. A mobile node is a node, for example, a personal digital assistant, a laptop computer, or a data-ready cellular phone, that can change its point of attachment from one network or subnet to another. This mobile node can travel from link to link and maintain ongoing communications while using the same IP address.

The Mobile Router functions similarly to the mobile node with one key difference—the Mobile Router allows entire networks to roam. For example, a plane with a Mobile Router can fly around the world while passengers stay connected to the Internet. This communication is accomplished by Mobile IP aware routers tunneling packets, which are destined to hosts on the mobile networks, to the location where the Mobile Router is visiting. The Mobile Router then forwards the packets to the destination device.

These devices can be mobile nodes running Mobile IP client software or nodes without the software. The Mobile Router eliminates the need for a Mobile IP client. In fact, the nodes on the mobile network are not aware of any IP mobility at all. The Mobile Router "hides" the IP roaming from the local IP nodes so that the local nodes appear to be directly attached to the home network.

The Cisco Mobile Networks feature is a static network implementation that supports stub routers only. The Mobile Router avoids convergence problems by statically defining which networks it can address. The Mobile Router can do the following:

- Perform agent solicitation
- Perform registration and reregistration
- Decapsulate information for its attached devices

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.htm.

Mobile Networks MIB Support

The Cisco Mobile Networks MIB Support feature implements mobile node MIB groups for the monitoring and management of Cisco Mobile Network activity. Data from managed objects is returned through the use of the "show" commands described in the documentation for the "Cisco Mobile Networks" 12.2(4)T feature, or can be retrieved from a Network Management System using SNMP.

The Cisco Mobile Networks MIB Support feature implements the following mobile node (mn) groups in the Mobile IP MIB (RFC2006-MIB): the mnSystem group, the mnDiscovery group, and the mnRegistrationGroup.

For further details, refer to the RFC2006-MIB.my file, available through Cisco.com at ftp://ftp.cisco.com/pub/mibs/v2/, and RFC 2206, "The Definitions of Managed Objects for IP Mobility Support using SMIv2."

MPLS Label Switch Controller and Enhancements

The Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC), combined with a slave ATM switch, supports scalable integration of IP services over an ATM network. The MPLS LSC enables the slave ATM switch to:

- Participate in an MPLS network
- Directly peer with IP routers
- Support the IP features in Cisco Internetwork Operating System (IOS) software

This feature was originally introduced in Cisco IOS Release 11.1CT as the Tag Switch Controller. Cisco IOS Release 12.2(4)T adds support for the following changes and additions:

- Changed tag-switching commands and terminology to MPLS format.
- Added support for Cisco MGX 8850 and 8950 switch with the Cisco MGX RPM-PR card as an MPLS LSC.
- Added DiffServ with MPLS QoS multi-VC feature support.
- Added the **vci-range** keyword to the **mpls atm vpi** and **mpls atm vp-tunnel** commands.
- Extended the VPI range from 256 to 4095.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmpls.htm.

MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels

Traffic engineering automatic bandwidth adjustment provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels based on their measured traffic load.

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, it periodically (for example, once per day) adjusts the tunnel's allocated bandwidth to be the largest sample for the tunnel since the last adjustment.

The frequency with which tunnel bandwidth is adjusted and the allowable range of adjustments is configurable on a per-tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate is user-configurable on a per-tunnel basis.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftbwadjm.htm.

MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion

The MPLS traffic engineering Internet Protocol (IP) explicit address exclusion feature provides a means to exclude a link or node from the path for an MPLS traffic engineering label-switched path (LSP).

The feature is accessible by the **ip explicit-path** command that allows you to create an IP explicit path and enter a configuration submode for specifying the path. The feature adds to the submode commands the **exclude-address** command for specifying addresses to exclude from the path.

If the exclude-address for an MPLS traffic engineering LSP identifies a flooded link, the constraint-based shortest path firs (CSPF) routing algorithm does not consider that link when computing paths for the LSP. If the exclude-address specifies a flooded MPLS traffic engineering router ID, the CSPF routing algorithm does not allow paths for the LSP to traverse the node identified by the router ID.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftaddexc.htm.

Multiservice Interchange (MIX) Support

On the Cisco 2600 series router, the Cisco 3620 router, and the Cisco 3640 router, MIX features are software only. On the Cisco 3660 router, MIX requires the installation of a multiservice interchange card, also called a MIX module (MIX-3660-64), which provides additional functionality.

MIX features support applications that are sensitive to time delay, such as voice and video. MIX enables the combination of different types of calls on a single T1 or E1 connection, giving customers the flexibility to manage traffic through their routers efficiently, as either traditional TDM connections or in packet-based format.

On Cisco 2600 series router, MIX allows connection of TDM streams between two voice/WAN interface cards (VWICs) on the same zero-LAN 2-slot network module (NM-2W).

On all Cisco 3600 series routers, MIX allows connection of TDM streams between two voice/WAN interface cards (VWICs) on the same Fast Ethernet network module (NM-xFE2W).

On the Cisco 3660 router, the MIX module also enables the following features:

- Connection of TDM streams between separate MIX-enabled network modules. The following network modules are currently MIX-enabled:
  - High-Density Voice (NM-HDV)
  - Fast Ethernet Mixed Media (NM-xFE2W)
  - ATM OC-3 CES (NM-1AOC3-XX-1V)
- DSP resource sharing across network modules, so that unused DSP resources on one network module (NM-HDV) can be configured to support voice traffic on other network modules (NM-xFE2W or NM-HDV).
- Circuit emulation of T1/E1s on Fast Ethernet Mixed Media cards (NM-xFE2W) and High-Density Voice network modules (NM-HDV) can now be supported by transporting them across MIX to ATM OC-3 network modules (NM-1AOC3-XX-1V).

The MIX feature also enhances extended availability drop and insert (EADI) functionality to ensure that TDM connections across slots survive a software reload if they have been saved in NVRAM. This means that the data or voice connections carried over TDM will survive even if the router goes down and comes back up again. No separate configuration is necessary for EADI, but to ensure that the TDM connections are not interrupted, their connect commands must be saved to NVRAM by writing the configuration. Other types of MIX connections, such as circuit emulation service (CES) connections and voice connections that terminate on the router, will not survive a software reboot or reload.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_24mix.htm.

NAT Support of H.323 RAS

The Cisco IOS NAT feature supports all H.225 and H.245 message types, including Registration, Admission, and Status (RAS). RAS provides a number of messages that are used by software clients and VoIP devices to register their location, request assistance in call setup, and control bandwidth. The RAS messages are directed toward an H.323 gatekeeper.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftnatras.htm.

NAT—Ability to Use Route Maps with Static Translations

The NAT—Ability to Use Route Maps with Static Translations feature provides support for NAT multihoming capability with static address translations. Support has been added for 1-to-1 static address translation only. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftnatrt.htm.

NAT—Static Mapping Support with HSRP for High Availability

The NAT—HSRP VMAC with NAT ARP Response feature allows NAT to use the HSRP Virtual MAC for ARPs. Failover is ensured without having to time out and repopulate upstream ARP caches. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftnthsrp.htm.

NAT—Translation of External IP Addresses Only

The NAT—Translation of External IP Addresses Only feature allows the configuration of Cisco IOS NAT to ignore all embedded IP addresses for any application and traffic type. It cannot be configured on a per application/traffic type basis. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftnatxip.htm.

NetFlow Multiple Export Destinations

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to the destination host. Currently, the maximum number of export destinations allowed is two.

The NetFlow Multiple Export Destinations feature improves the chances of receiving complete NetFlow data by providing redundant streams of data. Because the same export data is sent to more than one NetFlow collector, fewer packets will be lost.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/dtnfdest.htm.

NetFlow ToS-Based Router Aggregation

The NetFlow ToS-Based Router Aggregation feature provides the ability to enable limited router-based type of service (ToS) aggregation of NetFlow Export data, which results in summarized NetFlow Export data to be exported to a collection device. The result is lower bandwidth requirements for NetFlow Export data and reduced platform requirements for NetFlow data collection devices.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/dtnfltos.htm.

Offload Server Accounting Enhancement

The Offload Server Accounting Enhancement feature allows users to configure their access servers (NAS) to synchronize authentication and accounting information— NAS-IP-Address (attribute 4) and Class (attribute 25)—with the offload server.

An offload server interacts with an access server via Virtual Private Network (VPN) to perform required Point-to-Point Protocol (PPP) negotiation for calls. The NAS performs call preauthentication, while the offload server performs user authentication. Thus, this feature allows the authentication and accounting data of the NAS to synchronize with the offload server as follows:

- During preauthentication, the NAS generates a unique session-id, which adds the Acct-Session-Id (attribute 44) before the existing session-id (NAS-IP-Address), and retrieves a Class attribute. The new session-id is sent in preauthentication requests and resource accounting requests; the Class attribute is sent in resource accounting requests.

Note Note Unique session-ids are needed when multiple NASs are being processed by one offload server.

- The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted to the offload server via Layer 2 Forwarding (L2F) options.

The offload server will include the new, unique session-id in user access requests and user session accounting requests. The Class attribute that was passed from the NAS will be included in the user access request, but a new Class attribute will be received in the user access reply; this new Class attribute should be included in user session accounting requests.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftoffact.htm.

Optimized PPP Negotiation

The Optimized PPP Negotiation feature optimizes the time needed for PPP negotiation when a connection is made. PPP negotiation can include several cycles before the negotiation options are acknowledged. These negotiation cycles can cause a significant user-perceived delay, especially in networks with slow links such as a wireless data connection. Additionally, the PPP negotiation time can add significantly to the total time the user stays connected in these types of connections. Changes to the PPP link control protocol (LCP) and PPP Internet Protocol Control Protocol (IPCP) negotiation strategies as part of Cisco IOS Release 12.2(4)T make a reduction in the negotiation time possible.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftcphneg.htm.

OSPF ABR Type 3 LSA Filtering

The OSPF ABR Type 3 link-state advertisement (LSA) Filtering feature extends the ability of an ABR that is running the OSPF protocol to filter type 3 LSAs between different OSPF areas. This feature allows only specified prefixes to be sent from one area to another area and restricts all other prefixes.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftabrt3f.htm.

OSPF Stub Router Advertisement

The OSPF Stub Router Advertisement feature allows you to bring a new router into a network without immediately routing traffic through the new router and allows you to gracefully shut down or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration options that allow you to configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum or infinite metric to all neighbors.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftospfau.htm.

OSPF Update Packet-Pacing Configurable Timers

The OSPF Update Packet-Pacing Configurable Timers feature allows you to configure the rate at which Open Shortest Path First (OSPF) link-state advertisement (LSA) flood pacing, group pacing, and retransmission pacing updates occur. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftospfct.htm.

PIM MIB Extension for IP Multicast

Protocol Independent Multicast (PIM) is an IP Multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the *Protocol Independent Multicast for IPv4* MIB, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).

The PIM MIB Extension for IP Multicast feature introduces support in Cisco IOS software for the CISCO-PIM-MIB, which is an extension of RFC 2934 and an enhancement to the existing Cisco implementation of the PIM MIB. This feature introduces the following new classes of PIM notifications:

- neighbor-change—This notification results from the following conditions:
  - When the PIM interface of a router is disabled or enabled (using the **ip pim** command in interface configuration mode)
  - When the PIM neighbor adjacency of a router expires or is established (defined in RFC 2934)
- rp-mapping-change—This notification results from a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
- invalid-pim-message—This notification results from the following conditions:
  - When an invalid (*, G) join or prune message is received by the device (for example, when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group)
  - When an invalid PIM register message is received by the device (for example, when a router receives a register message from a multicast group for which it is not the RP)

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftpimmib.htm.

PPPoA/PPPoE Autosense for ATM PVCs

The PPPoA/PPPoE Autosense for ATM PVCs feature enables the router to distinguish between incoming PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE) over ATM sessions and to create virtual access based on demand for both PPP types.

The PPPoA/PPPoE Autosense for ATM PVCs feature is supported on LLC-encapsulated ATM PVCs only.

This new feature also adds support for precloning of virtual access interfaces for PPPoA and PPPoE over ATM. Precloning is the allocation of a specified number of virtual access interfaces at system start. Precloning significantly reduces the load on the system during call setup. When precloning is used, the virtual-access interface is attached to the permanent virtual circuit (PVC) upon receipt of the first PPP packet from the client on the PVC. The virtual-access interface is detached from the PVC on termination of the PPP session.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftp_auto.htm.

PPPoE over Gigabit Ethernet

The PPPoE over Gigabit Ethernet feature enhances PPP over Ethernet (PPPoE) functionality by adding support for PPPoE and PPPoE over IEEE 802.1Q VLANs on Gigabit Ethernet interfaces. The PPPoE over Gigabit Ethernet feature is supported on Cisco 7200 series routers with Gigabit Ethernet line cards.

PPPoE Session Limit

The PPPoE Session Limit feature enables you to limit the number of PPP over Ethernet (PPPoE) sessions that can be created on a router or on an ATM permanent virtual circuit (PVC), PVC range, or virtual circuit (VC) class.

This new feature introduces a new command and a modification to an existing command that enable you to specify the maximum number of PPPoE sessions that can be created. The new **pppoe limit max-sessions** command limits the number of PPPoE sessions that can be created on the router. The modified **pppoe max-sessions** command limits the number of PPPoE sessions that can be created on an ATM PVC, PVC range, VC class, or Ethernet subinterface.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftppoesl.htm.

PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer

The PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer feature fulfills the need for a standards based PRI Signaling backhaul that works with third party Call Agents to enable solutions like Integrated Access, IP PBX, and Telecommuter.

This feature provides the following:

- PRI Backhaul—Specific implementation for backhauling PRI.
- SCTP—New general transport protocol that can be used for backhauling signaling messages.
- IUA—Mechanism for backhauling any Layer 3 protocol that normally uses Q.921.

These features do the following:

- Provide a configuration interface for Cisco IOS software implementation.
- Implement the protocol message flows for SCTP and IUA.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_0546.htm.

PRI/Q.931 Signaling Backhaul for Call Agent Applications

This feature implements PRI/Q.931 signaling backhaul support for call agent applications on the Cisco 2600 and Cisco 3600 series routers and Cisco MC3810 series access concentrators. PRI/Q.931 signaling backhaul is the transport of PRI signaling (Q.931 and above layers) between a media gateway (such as a Cisco access server, router, or concentrator) and a media gateway controller (Cisco VSC3000).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_bhaul.htm.

PSTN Fallback for Cisco 7200 and 7500 Series Routers

The PSTN Fallback feature monitors congestion in the IP network and redirects calls to the PSTN or rejects calls on the basis of network congestion. The fallback subsystem has a network traffic cache that maintains the Calculated Planning Impairment Factor (ICPIF) or delay/loss values for various destinations. Performance is improved because each new call to a well-known destination does not have to wait on a probe to be admitted and the value is usually cached from a previous call.

This feature was originally introduced in Cisco IOS Release 12.1(3)T. With this release, support is added for the Cisco 7200 and 7500 series routers; the **call fallback** command is added, and the **call fallback reject cause code** command is added.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftpstn4t.htm.

RADIUS Attribute Screening

The RADIUS Attribute Screening feature allows users to configure a list of "accept" or "reject" RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.

If a NAS accepts and processes all RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers' authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftras.htm.

RADIUS Attribute 82: Tunnel Assignment ID

The RADIUS Attribute 82: Tunnel Assignment ID feature allows the Layer 2 Transport Protocol access concentrator (LAC) to group users from different per-user or domain RADIUS profiles into the same active tunnel. Previously, Cisco IOS software assigned a separate virtual private dialup network (VPDN) tunnel for each per-user or domain RADIUS profile, even if tunnels with identical endpoints already existed. The RADIUS Attribute 82: Tunnel Assignment ID feature defines a new AV pair, Tunnel-Assignment-ID, which allows the LAC to group users from different RADIUS profiles into the same tunnel if the chosen endpoint, tunnel type, and Tunnel-Assignment-ID are identical. This feature introduces new software functionality. No new commands are introduced with this feature.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftrada82.htm.

RADIUS Tunnel Preference for Load Balancing and Fail-Over

Tunnel servers may be load balanced or failed-over from a single tunnel initiator, as selected by the RADIUS Tunnel Preference for Load Balancing and Fail-Over attribute. There is no configuration associated with this feature. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftradtun.htm.

Redial Enhancements

The Redial Enhancements feature improves the performance of redial and provides greater control over redial behavior. The dialer will now cycle through all matching dialer strings or dialer maps before applying the redial interval, and may select a different physical dialer on each redial attempt. New dial-out attempts will not be initiated if a redial to the same destination is pending. The dialer can now be configured to apply a disable timer without performing any redial attempts, and a disable time can be applied to a dialer profile interface and to a serial dialer.

By default, the Cisco IOS software considers a call successful if it connects at the physical layer (Layer 1 of the Open System Interconnection [OSI] reference model). However, problems such as poor quality telco circuits or peer misconfiguration can cause dial-out failure even though a connection is made at tl physical layer. The Redial Enhancements feature introduces a new command that allows the router to be configured to wait a specific amount of time for a line protocol to come up before considering a dial-out attempt successful. If the timer runs out or the call is dropped before the line protocol comes up, the call is considered unsuccessful. Unsuccessful dial-out attempts will trigger redial if the redial options have been configured.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/dialenhc.htm.

RSVP Support for Low Latency Queueing

Resource Reservation Protocol (RSVP) is a network-control protocol that provides a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across networks achieve the desired quality of service (QoS).

RSVP enables real-time traffic (which includes voice flows) to reserve resources necessary for low latency and bandwidth guarantees.

Voice traffic has stringent delay and jitter requirements. It must have very low delay and minimal jitter per hop to avoid degradation of end-to-end QoS. This calls for an efficient queueing implementation, such as Low Latency Queueing (LLQ), that can service voice traffic at almost strict priority in order t minimize delay and jitter.

RSVP uses weighted fair queueing (WFQ) to provide fairness among flows and to assign a low weight to a packet to attain priority. However, the preferential treatment provided by RSVP is insufficient to minimize the jitter because of the nature of the queueing algorithm itself. As a result, the low latency and jitter requirements of voice flows might not be met in the prior implementation of RSVP and WFQ.

RSVP provides admission control. However, to provide the bandwidth and delay guarantees for voice traffic and get admission control, RSVP must work with LLQ. The RSVP support for LLQ feature allows RSVP to classify voice flows and queue them into the priority queue (PQ) within the LLQ system while simultaneously providing reservations for nonvoice flows by getting a reserved queue.

Sequential LRQ Enhancement

The Sequential LRQ Enhancement feature enhances the existing sequential location request (LRQ) feature in the Cisco IOS Gatekeeper (GK) to provide a potentially faster LRQ response to the originator of the request when a location reject (LRJ) response is received while the GK is sending sequential LRQs. In the current sequential LRQ implementation on the gateway, the GK sends an LRQ to the next zone only after the sequential delay timer expires. The Sequential LRQ Enhancement feature introduces a fixed delay for the GK to send sequential LRQs to successive zones even when a negative response or an LRJ is received from the current zone. If an LRJ is received from the current zone, the GK assumes that the current zone cannot satisfy the request and immediately sends an LRQ to the next zone. This feature works for both typical and directory GKs.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftseqlrq.htm.

SNMPv3 Community MIB Support

The SNMPv3 Community MIB Support feature implements support for the SNMP Community MIB (SNMP-COMMUNITY-MIB) module, defined in RFC 2576, in Cisco IOS software.

The SNMPv1/v2c Message Processing Model and Security Model require mappings between parameters used in SNMPv1 and SNMPv2c messages and the version independent parameters used in the Simple Network Management Protocol (SNMP) architecture. The SNMP Community MIB contains objects for mapping between these community strings and version-independent SNMP message parameters.

The mapped parameters consist of the SNMPv1/v2c community name and the SNMP securityName and contextEngineID/contextName pair. This MIB provides mappings in both directions, that is, a community name may be mapped to a securityName, contextEngineID, and contextName, or the combination of securityName, contextEngineID, and contextName may be mapped to a community name. This MIB also augments the snmpTargetAddrTable with a transport address mask value and a maximum message size value.

For implementation details, refer to the SNMP-COMMUNITY-MIB.my file, available through Cisco.com at ftp://ftp.cisco.com/pub/mibs/v2/.

SS7 Four-Link Support for Cisco Signaling Link Terminal

The SS7 Four-Link Support for Cisco Signaling Link Terminal feature introduces support for up to four Cisco SS7 links on a new platform for the Cisco SLT, the Cisco 2651 Multiservice Access Router. All existing Cisco 2611-based Cisco SLT functionality is supported on the new platform, and both Cisco SLT platforms use the same Cisco IOS software image.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_4lnk.htm.

Stream Control Transmission Protocol (SCTP), Release 1

Stream Control Transmission Protocol (SCTP) is a reliable datagram-oriented IP transport protocol, specified by RFC 2960. It provides the layer between an SCTP user application and an unreliable end-to-end datagram service such as IP. The basic service offered by SCTP is the reliable transfer of user datagrams between peer SCTP users. It performs this service within the context of an association between two SCTP hosts. SCTP is connection-oriented, but SCTP association is a broader concept than the Transmission Control Protocol (TCP) connection, for example.

SCTP provides the means for each SCTP endpoint to provide its peer with a list of transport addresses, such as address and UDP port combinations, for example. This list is provided during association startup and shows the transport addresses through which the endpoint can be reached and from which messages originate. The SCTP association includes transfer over all of the possible source and destination combinations that might be generated from the two endpoint lists (also known as multihoming).

SCTP is not explicitly configured on routers, but it underlies several Cisco applications. The commands described in this document are useful for troubleshooting when SCTP issues are suspected as the cause of problems.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_sctp.htm.

T.38 Fax Services for Cisco 1750 Access Routers

When the Cisco 1750 access router is equipped with a VFC that has one or more slots for voice interface cards (VICs), the Cisco 1750 access router supports carrier-class Voice over IP (VoIP) and fax over IP services. The VIC has Foreign Exchange Station (FXS), Foreign Exchange Office (FXO), and BRI interfaces.

Since the Cisco 1750 access router is H.323 compliant, it supports a family of industry-standard voice codecs and provides echo cancellation and voice activity detection (VAD) and silence suppression. There is an interactive voice response (IVR) application that provides voice prompts and digit collection in order to authenticate the user and identify the call destination.

The VIC is a coprocessor card with a powerful Reduced Instruction Set Computer (RISC) engine and dedicated, high-performance digital signal processors (DSPs) modules to ensure predictable, real-time voice processing. The design enables streamlined packet forwarding. The Cisco 1750 access router supports one VIC with two voice ports.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftfaxrly.htm.

Timer and Retry Enhancements for L2TP and L2F

The L2TP & L2F Timer/Retry Enhancement feature allows the user to configure certain adjustable timers for the Layer 2 Tunnel Protocol (L2TP) and Layer 2 Forwarding (L2F) protocols. For L2F, the settings for control packet retries and control packet timeouts are now both configurable. Initial tunnel packet retries and initial tunnel packet timeouts are now configurable for both the L2F and L2TP protocols.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftretreh.htm.

Two-Rate Policer

Networks police traffic by limiting the input or output transmission rate of a class of traffic based on user-defined criteria. Policing traffic allows you to control the maximum rate of traffic sent or received on an interface, and to partition a network into multiple priority levels or class of service (CoS).

The Two-Rate Policer performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria.
- Marks packets by setting the ATM Cell Loss Priority (CLP) bit, Frame Relay Discard Eligibility (DE) bit, IP precedence value, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, and Quality of Service (QoS) group.

With the Two-Rate Policer, you can enforce traffic policing according to two separate rates—committed information rate (CIR) and peak information rate (PIR). You can specify the use of these two rates, along with their corresponding values, by using two keywords, **cir** and **pir**, of the **police** command. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft2rtplc.htm.

TX Ring Adjustment

Each permanent virtual circuit (PVC) has a hardware transmit queue, or TX ring. It is a simple FIFO queue, and on the c820 it has a default size of 16 packets. This feature allows adjustment of the size of the TX ring. If both voice and data packets are transmitted on the same PVC, the length of the TX ring must be reduced to a value of about 3 packets. This reduces delay and jitter for voice packets by decreasing the maximum number of data packets or fragments that can be in front of a voice packet inside the TX ring.

Using 31-Bit Prefixes on IPv4 Point-to-Point Links

The Using 31-Bit Prefixes on IPv4 Point-to-Point Links feature allows 31-bit prefixes to be used on IP version 4 point-to-point links. The number of IP addresses is reduced by 50 percent and the number of denial of service (DoS) attacks is also reduced. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft31addr.htm.

VPDN Group Session Limiting

Before the introduction of the VPDN Group Session Limiting feature, you could only globally limit the number of Virtual Private Dialup Network (VPDN) sessions on a router with limits applied equally to all VPDN groups. Using the VPDN-Group Session Limiting feature, you can limit the number of VPDN sessions allowed per VPDN group. This feature is implemented with the introduction of the **session-limit** *number* command in VPDN group configuration mode. VPDN group session limiting is applied after the global VPDN session limiting (which is configured via the **vpdn session-limit** *session* command in configuration mode) is enforced.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftvpdngs.htm.

Hardware Platforms and Modules Newly Supported in Cisco IOS Release 12.2(2)T

The following hardware platforms and modules are now supported in Cisco IOS Release 12.2(2)T. These platforms and modules were first introduced in earlier Cisco IOS software releases.

1-Port ADSL WAN Interface Card

The ADSL WAN interface card is a 1-port WAN interface card (WIC) for the Cisco 1700 series of modular access routers. The card provides asymmetric digital subscriber line (ADSL) high-speed digital data transfer between a single customer premises equipment (CPE) subscriber and the central office.

The ADSL WIC is compatible with the Alcatel Digital Subscriber Loop Access Multiplexer (DSLAM), the Cisco 6260 DSLAM with Flexi-line cards, and the Cisco 6130 DSLAM with Flexi-line cards. It supports ATM adaptation layer (AAL5) and various classes of quality of service (QoS) for both voice and data service.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/wan_mod/index.htm.

ADSL over ISDN

Cisco 826 routers connect corporate telecommuters and small offices via Internet Service Providers (ISPs) over asymmetric digital subscriber lines (ADSLs) to corporate LANs and the Internet. The router can provide bridging and multiprotocol routing between LAN and WAN ports. Cisco 826 routers provid connectivity to an ISDN network through an ADSL port.

Cisco uBR905 Cable Access Router

The Cisco uBR905 Cable Access Router features a single F-connector interface to the cable system, four RJ-45 (10BASE-T Ethernet) hub ports, and one RJ-45 console port to connect to a laptop computer/console terminal for local Cisco IOS configuration. The Cisco uBR905 Cable Access Router also provides an onboard IPSec hardware accelerator, which provides high-performance encryption that is substantially faster than software-based encryption.

Small Office, Home Office ADSL Router

Cisco IOS Release 12.2 T supports the following Cisco SOHO series routers:

- SOHO 76
- SOHO 77

The SOHO 76 and SOHO 77 are small office, home office (SOHO) asymmetric digital subscriber line (ADSL) routers, each with one Ethernet interface for connection to service provider networks.

The SOHO routers also provide the following key hardware features:

- Connection to an ADSL network through an ADSL port.
- A central processing unit: 50 MHz MPC 855T RISC processor.
- Ability to be stacked or mounted on a wall.
- Locking power connectors and a Kensington-compatible locking slot.

WT-2750 Multipoint Broadband Wireless System

The Cisco broadband fixed wireless point-to-multipoint system is an integrated solution consisting of one headend (WT-2751 Multipoint Headend Line Card) and multiple subscriber units (WT-2755 Multipoint Subscriber Network Module). The fixed wireless point-to-multipoint subscriber unit is designed to receive radio frequency (RF) signals from the headend. It also transmits a return signal to the headend. This return signal is a point-to-point signal, so a properly installed subscriber antenna must be correctly oriented with the headend antenna to which it is transmitting.

For more information about the fixed wireless point-to-multipoint headend feature, see *Point-to-Multipoint Support for the Cisco uBR7200 Series Universal Broadband Router* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/bbfw/p2mp/index.htm.

The fixed wireless multipoint system incorporates Vector Orthogonal Frequency Division Multiplexing (VOFDM), so it does not always depend on line-of-sight (LOS) deployment. With VOFDM, the system allows wireless operation in obstructed, non-line-of-sight (non-LOS) environments by taking advantage of multipath signals. This can be particularly useful in urban and suburban environments.

Wireless Network Module

The NM-WMDA wireless network module installs in the network module slot of a Cisco 2600 series router. Installing a wireless network module enables the Cisco 2600 series router to act as a subscriber unit (SU) in a point-to-multipoint wireless network. It is configured through the router's system console or via the CiscoView network management system. The network module provides the control and data interface between the Cisco 2600 series digital motherboard and the radio frequency (RF) subsystem in the wireless transverter. It also provides the up/down conversion from baseband to intermediate frequency (IF). One network module supports one or two wireless transverters (main and diversity).

Microcode software images ship in Flash memory along with the system software image. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface line cards.

It is possible to use a later version of microcode software than the one shipped with the Cisco IOS software from the factory. The microcode software in Flash memory is mapped to the line cards. Unless you fully understand how Cisco IOS software uses microcode software, it is important to keep the factory configuration.

The multipoint wireless modem card requires external microcode software. Information about this microcode software is available (with a Cisco.com login) at the following location:

http://www.cisco.com/cgi-bin/tablebuild.pl/rsu.

For further information regarding the network module, refer to the *Cisco Network Modules Hardware Installation Guide* (for Cisco 2600 series routers) for detailed installation instructions, and the *Software Configuration Guide* (for Cisco 2600 series routers) for an overview of network module configuration procedures and information on configuring specific network modules.

New Software Features in Cisco IOS Release 12.2(2)T

The following new features are supported in Cisco IOS Release 12.2(2)T. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

56K CSU Support for the Cisco Signaling Link Terminal

This feature module verifies support for the WIC-1DSU-56K4 WAN interface card for support of DS0 interconnect by the Cisco Signaling Link Terminal (SLT).

The addition of the WIC-1DSU-56K4 support to the Cisco SLT provides support for DS0 interconnect to the SS7 network without the need for an external CSU/ DSU. The WIC-1DSU-56K4 interface card is a single-port serial interface card providing a 4-wire, 56/64-kbps Kb/s interface with an integrated onboard CSU/DSU. This card is a standard option for the Cisco 2600 series routers.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftsltwic.htm.

Analog DID for Cisco 2600 and Cisco 3600 Series Routers

Direct Inward Dialing (DID) is a service offered by telephone companies that enables callers to dial directly to an extension on a PBX without the assistance of an operator or automated call attendant. This service makes use of DID trunks, which forward only the last three to five digits of a phone number to the PBX. If, for example, a company has a PBX with extensions 555-1000 to 555-1999, and a caller dials 555-1234, the local CO would forward 234 to the PBX. The PBX would then ring extension 234. This entire process is transparent to the caller.

When this feature is configured, a voice-enabled Cisco 2600 and Cisco 3600 series router can receive calls from a DID trunk and connect them to the appropriate extensions. The DID state machine is identical to the E&M state machine and uses one of the following signaling types:

- Immediate start—The originating end seizes the line by going off-hook and, without waiting for a response, it begins to outpulse digits. The address signaling used with immediate-start signaling consists only of dial-pulsing.
- Wink-start—The originating end seizes the line by going off-hook. It waits for acknowledgement from the other end before outpulsing digits. The acknowledgement serves as an integrity check that will identify a malfunctioning trunk and allow the network to send a reorder tone to the calling party.
- Delay dial—The originating end seizes the line and waits 200 ms to see if the far end is on-hook. If so, the originating end then outpulses digits. If the far end is off-hook, the originating end waits until the far end is on-hook before outpulsing digits.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/dt_did.htm.

ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping

In a digital subscriber line (DSL) environment, many applications require the configuration of a large number of ATM permanent virtual circuits (PVCs). The ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping feature enables you to group a number of PVCs into a PVC *range* in order to configure them all at once.

For applications that use multipoint subinterfaces, such as PPP over Ethernet and PPP over ATM, the PVC range is on a single multipoint subinterface. For applications that use point-to-point subinterfaces, such as routed bridge encapsulation (RBE), a point-to-point subinterface is created for each PVC in the range.

A PVC range is defined by two VPI-VCI pairs. The two virtual path identifiers (VPIs) define a VPI range, and the two virtual channel identifiers (VCIs) define a VCI range. The number of PVCs in the PVC range equals the number of VPIs in the VPI range multiplied by the number of VCIs in the VCI range.

Once the PVC range is defined, you can configure the range by using the existing interface-ATM-VC configuration commands that are also supported in ATM PVC range configuration mode. The **shutdown** ATM PVC range configuration mode command can be used to deactivate the range without deleting the configuration.

The ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping feature also introduces the **pvc-in-range** command, which allows you to explicitly configure an individual PVC within the defined range of PVCs on a multipoint subinterface. The **shutdown** ATM PVC-in-range configuration mode command allows you to deactivate an individual PVC within a range.

Note You cannot explicitly configure the individual point-to-point subinterfaces created by the PVC range on a point-to-point subinterface. All of the point-to-point subinterfaces in the range share the same configuration as the subinterface on which the PVC range is configured.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtatmpvr.htm.

BGP Link Bandwidth

The Border Gateway Protocol (BGP) Link Bandwidth feature is used to advertise the bandwidth of an autonomous system exit link as an extended community. The BGP Link Bandwidth feature is supported by the internal BGP (iBGP) and external BGP (eBGP) multipath features. The link bandwidth extended community indicates the preference of an autonomous system exit link in terms of bandwidth. The link bandwidth extended community attribute may be propagated to all iBGP peers and used with the BGP multipath features to configure unequal cost load balancing. When a router receives a route from a directly connected external neighbor and advertises this route to iBGP neighbors, the router may advertise the bandwidth of that link.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftbgplb.htm.

Circuit Interface Identification Persistence for SNMP

The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object (cciDescr) that can be used to identify individual circuit-based interfaces for SNMP monitoring. The Circuit Interface Identification Persistence for SNMP feature maintains this user-defined name of the circuit across reboots, allowing the consistent identification of circuit interfaces. Circuit Interface Identification Persistence is enabled using the **snmp mib persist circuit** global configuration command.

Cisco High-Performance Gatekeeper

The Cisco High-Performance Gatekeeper feature introduces new gatekeeper functionality and modifications for facilitating carrier class reliability, security, and performance into Cisco's Voice Network solution portfolio. These H.323 standard-based features have carrier grade reliability and performance characteristics with a robust open application protocol interface to enable development of enhanced applications like voice Virtual Private Networks (VPNs) and wholesale voice solutions.

The new gatekeeper is characterized by the following:

- Increased support for back end applications.
- Increased performance on a single gatekeeper.

- Alternate gatekeeper support to the gatekeeper. Each alternate gatekeeper, or GK node, shares its local zone information so that the cluster can effectively manage all local zones within the cluster. Each alternate gatekeeper has a unique local zone. Clusters provide a mechanism for distributing call processing seamlessly across a converged IP network infrastructure to support IP telephony, facilitate redundancy, and provide feature transparency and scalability.

This feature addresses the scalability, redundancy, and performance aspects of the gatekeeper as part of the Cisco Multimedia Conference Manager (MCM) to present a complete Cisco solution. The Cisco H.323 MCM provides the network administrator with the ability to identify H.323 traffic and to apply appropriate policies. The Cisco H.323 Multimedia Conference Manager is implemented on Cisco IOS software and enables a network manager to do the following:

Limit the H.323 traffic on the LAN and WAN.

Provide user accounting for records based on the service utilization.

Inject quality of service (QoS) parameters for the H.323 traffic generated by applications such as VoIP, and data and video conferencing.

Provide the mechanism to implement security for H.323 communications.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ft_0394.htm.

Cisco IOS Server Load Balancing

The IOS SLB feature is a Cisco IOS-based solution that provides IP server load balancing. Using the IOS SLB feature, the network administrator defines a virtual server that represents a group of real servers in a cluster of network servers known as a server farm. In this environment the clients are configured to connect to the IP address of the virtual server. The virtual server IP address is configured as a loopback address, or secondary IP address, on each of the real servers. When a client initiates a connection to the virtual server, the IOS SLB function chooses a real server for the connection based on a configured load-balancing algorithm.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/iosslb5t.htm.

Cisco Signaling Link Terminal G.732 Support

The addition of ITU-T G.732 support to the Cisco Signaling Link Terminal (SLT) is a fundamental requirement for passing homologation in many European countries. As an integral part of the Cisco Signaling Controller 2200 (SC2200) and the Cisco VSC3000 Virtual Switch Controller (VSC3000) architecture, the Cisco SLT provides the Cisco Signaling System 7 (SS7) connectivity into the SC or VSC node.

The Cisco SLT enables service providers to reliably transport Signaling System 7 (SS7) protocols across an IP network. The Cisco SLT uses the Cisco IOS SS7 SLT feature set, providing reliable interoperability with the Cisco SC2200 or the Cisco VSC3000. The Cisco SLT is responsible for terminating the Message Transfer Part (MTP) 1 and MTP 2 layers of the SS7 protocol stack. Using the Cisco Reliable User Datagram Protocol (RUDP), the Cisco SLT backhauls, or transports, upper-layer SS7 protocols across an IP network to the Cisco SC2200 or the Cisco VSC3000. The Cisco SLT is supported only on the Cisco 2611 router.

ITU-T G.732 is an extract from the ITU-T blue book describing characteristics of primary Pulse Code Modulation (PCM) multiplex equipment operating at 2048 kbit/s (E1). The requirements describing excessive bit error ratios detected by monitoring the frame alignment signal (loss of frame alignment fault conditions) and subsequent alarming actions relate to the Cisco SLT.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft_g732.htm.

Cisco Quality of Service Device Manager 2.0 Support for Cisco 1700 Series Routers

QDM is now supported on Cisco 1700 series routers.

Cisco Quality of Service Device Manager (QDM) is a web-based Java application with which users can configure and monitor advanced IP-based Quality of Service (QoS) functionality within Cisco routers using a graphical user interface (GUI).

QDM 2.0 is available as a separate product download and is free of charge. If you would like to install or reinstall QDM, refer to the Release and Installation Notes for Cisco Quality of Service Device Manager 2.0 on Cisco.com and the Documentation CD-ROM for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/qdm/qdmrn20.htm.

Class-Based Marking

The Class-Based Packet Marking feature provides users with a user-friendly command-line interface (CLI) for efficient packet marking by which users can differentiate packets based on the designated markings. The Class-Based Packet Marking feature allows users to perform the following tasks:

- Mark packets by setting the IP precedence bits or the IP differentiated services code point (DSCP) in the IP type of service (ToS) byte.
- Mark packets by setting the Layer 2 Class of Service (CoS) value.
- Associate a local quality of service (QoS) group value with a packet.
- Set the Cell Loss Priority (CLP) bit setting in the ATM header of a packet from 0 to 1.
- Set the Frame Relay Discard Eligibility (DE) bit in the address field of the frame relay frame from 0 to 1.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/cbpmark2.htm

Note This feature was originally introduced in Cisco IOS Release 12.1(2)T as QoS Packet Marking. Cisco IOS Release 12.2(2)T introduces the **set fr-de** command.

Classifying VoIP Signaling and Media with DSCP for QoS

The Classifying VoIP Signaling and Media with DSCP for QoS feature introduces the **ip qos dscp** command. The **ip precedence** command in dial-peer configuration mode, was originally designed to allow the prioritizing of H.323 traffic and the priority used, typically higher than that of IP data traffic. There was no means, however, for the end user to configure prioritization of H.245, H.225, and SIP signaling packets, which resulted in a delay when a call was set up over a congested network.

In order to provide finer tuning of priorities, the **ip precedence** command has been replaced by the **ip qos dscp** command. If a non zero value is specified for a particular type of traffic stream, this value is stored in the DSCP (Differentiated Services Code Point) before the gateway sends the packet out its WAN interface.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft_dscp.htm.

CNS Configuration Agent

CNS is a foundation technology for linking users to network services. CNS SDK accomplishes this by making applications network-aware and increasing the intelligence of the network elements. CNS SDK provides building blocks to a range of customers in market segments such as Enterprise, service provider, independent software vendors, and system integrators.

The CNS Configuration Agent supports routing devices by providing:

- Initial configurations
- Incremental (partial) configurations
- Synchronized configuration updates

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcns_ca.htm.

CNS Event Agent

CNS is a foundation technology for linking users to network services. CNS SDK accomplishes this by making applications network-aware and increasing the intelligence of the network elements. CNS SDK provides building blocks to a range of customers in market segments such as Enterprise, service provider, independent software vendors, and system integrators.

The CNS Event Agent is part of the Cisco IOS infrastructure that allows Cisco IOS applications, for example CNS Configuration Agent, to publish and subscribe to events on a CNS Event Bus. CNS Event Agent works in conjunction with CNS Configuration Agent.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcns_ea.htm.

Control Plane DSCP for RSVP

The Control Plane DSCP Support for RSVP feature allows you to set the priority value in the type of service (ToS) byte/differentiated services (DiffServ) field in the IP header for RSVP signaling messages. The IP header functions with resource providers such as weighted fair queueing (WFQ), so that voice frames have priority over data fragments and data frames. When packets arrive in a router output queue, the voice packets are placed ahead of the data frames.

There is one new command:

ip rsvp signalling dscp [value]–Specifies the DSCP to be used on all RSVP messages sent on an interface.

There is one modified command:

show ip rsvp interface detail—The detail keyword, was added to display information about RSVP interface parameters.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/dscprsvp.htm.

DF Bit Override Functionality with IPSec Tunnels

The DF Bit Override Functionality with IPSec Tunnels feature allows customers to configure the setting of the DF bit when encapsulating tunnel mode IPSec traffic on a global or per-interface level. Thus, if the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting. Refer to the following document for additional information:

http:/www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftdfipsc.htm.

DFP Support in DistributedDirector

DistributedDirector can obtain load information from Cisco LocalDirector, Catalyst 4840g, and other clients using Dynamic Feedback Protocol (DFP). This protocol allows the user to configure the DistributedDirector to communicate with various DFP agents. The DistributedDirector tells the DFP agents how often they should report load information; then the DFP agent can tell the DistributedDirector which LocalDirector cluster to remove from providing service.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/distrdir/dtdddfp.htm.

DHCP Option 82 Support for Routed Bridge Encapsulation

The DHCP Option 82 Support for Routed Bridge Encapsulation feature provides support for the DHCP relay agent information option when ATM routed bridge encapsulation (RBE) is used.

This feature enables the DHCP relay agent to communicate information to the DHCP server using a suboption of the DHCP relay agent information option called agent remote ID. The information sent in agent remote ID includes an IP address identifying the relay agent and information about the ATM interface and the PVC over which the DHCP request came in. The DHCP server can use this information to make IP address assignments and security policy decisions.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftrbeo82.htm.

Distributed Time-Based Access Lists

Cisco IOS software allows implementation of access lists based on the time of day. To do the implementation, you create a time range that defines specific times of the day and week. The time range is identified by a name and then referenced by a function, so that those time restrictions are imposed on the function itself.

Before the introduction of the Distributed Time-Based Access Lists feature, time-based access lists were not supported on line cards for the Cisco 7500 series routers. If time-based access lists were configured, they behaved as normal access lists. If an interface on a line card was configured with access lists, the packets switched into the interface were not distributed switched through the line card but forwarded to the Route Processor for processing.

The Distributed Time-Based Access Lists feature allows packets destined for an interface configured with time-based access lists to be distributed switched through the line card.

The Distributed Time-Based Access Lists feature gives network administrators more control over permitting or denying a user access to resources. Customers can now take advantage of the performance benefits of distributed switching and the flexibility given by time-based access lists.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftdistac.htm.

DNS Server Support for NS Records

DistributedDirector has improved server load-balancing capacity with the Domain Name System (DNS) Server Support for Name Server (NS) Records feature. This feature adds support for NS records to the Cisco IOS DNS server. With this feature, the DistributedDirector can distribute the server-selection process to multiple DistributedDirectors, improving overall server capacity.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftddns.htm.

Enhanced Multilingual Support for Cisco IOS Integrated Voice Response

This feature releases the infrastructure to support Tool Command Language (TCL)-based script interpreters, which allow you to easily add new languages to your router or access server. You can add a new language by creating a TCL script that interprets prompts into a sequence of audio files or silences. The underlying Cisco IOS dynamic prompting code interfaces with the TCL script to translate the message into a sequence of URLs that point to audio files. Then, the Cisco IOS software plays the sequence of audio files as a dynamic prompt. New TCL-script language interpreters operate simultaneously with the current built-in languages: Spanish, Chinese/Mandarin, and English. Adversely, new TCL-script language interpreters can replace one or more of the built-in languages by overwriting the built-in language functionality.

Note This feature does not release any specific TCL scripts.

Note Although the language intelligence comes from a TCL-based language script, once you configure a language any system (TCL IVR 1.0, 2.0, VxML, MGCP, and so on) on your router can use the configured language with little to no change to Cisco IOS Software.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmultil.htm.

Firewall Feature Set for Cisco 820 Series Routers

The Cisco IOS Firewall feature set is available on the Cisco 820 series routers. This feature set provides the following capabilities:

- Context-Based Access Control (CBAC)
- Java blocking
- Denial-of-service detection and prevention
- Real-time alerts and audit trails

The Cisco IOS Firewall Feature Set feature module provides several sample firewall configurations, including the following examples for small-office environments:

- IP network to Internet
- Remote office network to corporate office network

Frame Relay Discard Eligibility Bit Setting

The Modular QoS CLI in Cisco IOS Release 12.2(2)T has been enhanced to include matching and marking based on the Frame Relay Discard Eligibility (DE) bit. Frame Relay DE bit Matching and Marking is documented as part of the Class-Based Marking feature module.

The DE bit in the address field of a Frame Relay frame is used as a method for prioritizing the discarding of frames in congested frame relay networks. The Frame Relay DE bit has only one bit and can therefore only have two settings, 0 or 1. If congestion occurs in a Frame Relay network, frames with the DE bit set at 1 are discarded before frames with the DE bit set at 0. Therefore, important traffic should have the DE bit set at 0 and less important traffic should be forwarded with the DE bit set at 1.

The default DE bit setting is 0. The Class-Based Packet Marking feature allows users to change the DE bit setting to 1 for various traffic, giving users the option of keeping the default value of 0 or changing the value to 1. Users can therefore use the Frame Relay DE bit marking to prioritize frames in a Frame Relay network.

Frame Relay Point-Multipoint Wireless

This feature provides an end-to-end frame relay network for customers using wireless interfaces in their frame relay network. Several new commands are used to establish a virtual frame relay interface, then link it to a specific multipoint destination mac address. The configuration information is associated with a new interface type, virtual frame relay and new interface commands, **interface virtual-framerelay** and **frame relay over radio**.

Using the new interface enables Cisco uBR7200 series, Cisco 3600 and Cisco 2600 routers to provide a seamless transition from a serial interface to a multipoint frame relay interface. By implementing RFC 1315, Frame Relay DTE MIB, a virtual frame relay interface can be linked to a specific multipoint radio interface and destination MAC address. The headend (HE) router acts as a frame relay switch, receiving radio frequency signals from subscriber units. Once received, the multipoint link is switched to a serial link and then to an upstream router.

Functionality Changed for the tunnel mpls traffic-eng autoroute metric Command

The default behavior of the **tunnel mpls traffic-eng autoroute metric** interface configuration command has been changed in Cisco IOS Release 12.2(2)T. This command now combines the costs of all Intermediate-System to Intermediate-System (IS-IS) routes that are downstream from a Traffic Engineering (TE) tunnel into an additive path metric. IS-IS uses the additive path metric to set the metric of the TE tunnel.

FXO Answer and Disconnect Supervision

The FXO Answer and Disconnect Supervision feature enables analog FXO ports to monitor call-progress tones, and to monitor voice and fax transmissions returned from a PBX or from the PSTN.

You can configure voice ports to detect either the standard call-progress tones that are preconfigured for certain countries, or you can configure custom call-progress tone detection. Tone detection is performed by the digital signal processor (DSP) and causes a DSP event to be reported to the host software.

Answer supervision can be accomplished in two ways: by detecting battery reversal, or by detecting voice, fax, or modem tones. If an FXO voice port is connected to the PSTN, and battery reversal is supported, use the battery reversal method. Voice ports that do not support battery reversal must use the answer supervision method, in which answer supervision is triggered when the DSP detects voice, modem, or fax transmissions. Configuring answer supervision automatically enables disconnect supervision; however, you can configure disconnect supervision separately if answer supervision is not configured.

Disconnect supervision can be configured to detect call-progress tones sent by the PBX or PSTN (for example, busy, reorder, out-of-service, number-unavailable), or to detect any tone received (for example, busy tone or dial tone). When an incoming call ends, the DSP detects the associated call-progress tone, causing the analog FXO voice port to go on-hook.

You can configure disconnect tones to be detected either continuously during calls or only during call setup (before calls are answered). Detection of any tone operates only during call setup. If you configure detection of any tone, you must also enable echo cancellation to prevent disconnection due to detection of the ringback tone of the router.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft_ansds.htm.

H.323 Call Redirection Enhancements

The user-to-user information element (UUIE) of the Facility message is used primarily for call redirection. The UUIE contains a field, facilityReason, that indicates the nature of the redirection. The H.323 Call Redirection Enhancements feature adds support for two of the reasons: routeCallToGatekeeper and callForwarded. It also provides a nonstandard method for using the Facility message to effect call transfer.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcallrd.htm.

H.323 Version 2 Phase 2

Cisco H.323 Version 2 Phase 2 upgrades Cisco IOS software by adding the following optional features, and facilitates customized extensions to the Cisco gatekeeper:

- H.323v2 Fast Connect
- H.245 Tunneling of DTMF Relay in conjunction with Fast Connect
- H.450.2 Call Transfer
- H.450.3 Call Deflection
- Translation of FXS Hookflash Relay
- H.235 Security
- Gatekeeper Transaction Message Protocol (GKTMP) and RAS Messages
- Gatekeeper and Alternate Endpoints
- Gatekeeper C Code Generic API for GKTMP in a UNIX Environment
- Gateway Support for Network-Based Billing Number

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/h323v2p2.htm

High-Performance Gatekeeper

The Cisco High-Performance Gatekeeper feature introduces new gatekeeper functionality and modifications for facilitating carrier class reliability, security, and performance into the Cisco voice network solution portfolio. These H.323 standard-based features have carrier grade reliability and performance characteristics with a robust open application protocol interface to enable development of enhanced applications like voice VPNs and wholesale voice solutions.

This feature addresses the scalability, redundancy, and performance aspects of the gatekeeper as part of the Cisco Multimedia Conference Manager (MCM) to present a complete Cisco solution. The Cisco H.323 MCM provides the network administrator with the ability to identify H.323 traffic and to apply appropriate policies.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ft_0394.htm.

iBGP Multipath Load Sharing

When a Border Gateway Protocol (BGP) speaker router with no local policy configured receives multiple network layer reachability information (NLRI) from the internal BGP for the same destination, the router will choose one internal BGP path as the best path. The best path is then installed in the IP routing table of the router.

The Internal BGP Multipath Load Sharing feature enables the BGP speaker router to select multiple internal BGP paths as the best paths to a destination. The best paths or multipaths are then installed in the IP routing table of the router.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftbgpls.htm.

Interactive Voice Response Version 2.0 on Cisco VoIP Gateways

IVR Version 2.0 is the fourth release of IVR and TCL scripting on Cisco IOS VoIP gateways. The Cisco IVR feature (first made available in Cisco IOS Release 12.0(3)T and 12.0(7)T) provides IVR capabilities using TCL scripts.

IVR is a term that is used to describe systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words, or more commonly dual tone multifrequency (DTMF) signaling. For example, when a user makes a call with a debit card, an IVR application is used to prompt the caller to enter a specific type of information, such as a PIN. After playing the voice prompt, the IVR application collects the predetermined number of touch tones (digit collection), forwards the collected digits to a server for storage and retrieval, and then places the call to the destination phone or system. Call records can be kept and a variety of accounting functions performed.

The IVR application (or script) is a voice application designed to handle calls on a voice gateway, which is a router that is equipped with Voice over IP (VoIP) features and capabilities.

The IVR feature allows an IVR script to be used during call processing. The scripts interact with the IVR software to perform the various functions. Typically, IVR scripts contain both executable files and audio files that interact with the system software.

IVR Version 2.0 is made up of several separate components in the section that follows. These new features include:

- Media Gateway Control Protocol (MGCP) scripting package implementation
- Real Time Streaming Protocol (RTSP) client implementation
- New Tool Command Language (TCL) verbs to utilize RTSP and MGCP scripting features
- IVR prompt playout and digit collection on IP call legs
- Performance improvements and TCL infrastructure changes
- IVR application MIB for network management

These features add scalability and enable the IVR scripting functionality on VoIP call legs. In addition, support for RTSP enables VoIP gateways to play messages from RTSP-compliant announcement servers.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/12_2t/pulskynx.htm.

Interface Alias Long Name Support

The Interface Alias (ifAlias) is a user-specified description of an interface used for SNMP network management. The ifAlias is an object in the Interfaces Group MIB (IF-MIB), which can be set by a network manager to "name" an interface. The ifAlias value for an interface or subinterface can be set using the **description** command in interface configuration mode, or by using a Set operation from a Network Management System.

Prior to the Cisco IOS Release 12.2(2)T, ifAlias descriptions for subinterfaces were limited to 64 characters. A new Cisco IOS software command, **snmp ifmib ifalias long**, configures the system to handle ifAlias descriptions of up to 256 characters. IfAlias descriptions appear in the output of the **show interfaces** CLI command.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftshowif.htm.

Interface Index Display

The Interface Index (IfIndex) is a user-specified identification number for an interface used in SNMP network management. The IfIndex is an object in the Interfaces Group MIB (IF-MIB), which can be set by a network manager to consistently identify an interface. A new Cisco IOS software command, **show snmp mib ifmib ifindex**, allows the user to display the IfIndex identification numbers assigned to interfaces and subinterfaces using the CLI. The IFIndex provides a way to display these values without the need for a Network Management Station.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftshowif.htm.

IP Header Compression Enhancement—PPPoATM and PPPoFR Support

In Cisco IOS Release 12.2(2)T, IP header compression (TCP and IP/UDP/RTP) is now supported on PPP-over-ATM interfaces and PPP-over-Frame Relay interfaces. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/fqcprt6/qcflem.htm.

IPSec and 3DES Feature Set for Cisco 820 Series Routers

The Internet Protocol Security (IPSec) feature is available on the Cisco 820 series routers. IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following standards:

- IPSec
- Internet Key Exchange (IKE)
- Data Encryption Standard (DES)
- Message Digest 5 (MD5)
- Secure Hash Algorithm (SHA)
- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

IPSec services are similar to those provided by Cisco Encryption Technology (CET), a proprietary security solution introduced in Cisco IOS Release 11.2. (The IPSec standard was not yet available at Release 11.2.) It provides network data encryption at the IP packet level and implements the following standards:

- Digital Signature Standard (DSS)
- Diffie-Hellman (DH) public key algorithm
- Data Encryption Standard (DES)

IPSec provides a more robust security solution and is standards-based. IPSec also provides data authentication and antireplay services in addition to data confidentiality services, and CET provides only data-confidentiality services.

The following component technologies are implemented for IPSec:

- DES is used to encrypt packet data.
- Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.
- MD5 and SHA are hash algorithms.

Triple Data Encryption Standard Feature Set for Cisco 820 Series Routers

The Triple Data Encryption Standard (3DES) Cisco IOS feature is available on Cisco 820 series routers. This feature encrypts packet data. Cisco IOS software implements the mandatory 56-bit DES-Cipher Block Chaining (CBC) with an Explicit initialization vector (IV).

IPv6 for Cisco IOS Software

IPv6, formerly called IPng (next generation), is the latest version of IP that offers many benefits, such as a larger address space, over the previous version of IP (version 4). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/index.htm.

Low Latency Queueing with Priority Percentage Support

This feature allows you to configure bandwidth as a percentage within low latency queueing (LLQ). Specifically, you can designate a percentage of the bandwidth to be allocated to an entity (such as a physical interface, a shaped ATM permanent virtual circuit (PVC), or a shaped Frame Relay PVC) to which a policy map is attached. Traffic associated with the policy map will then be given priority treatment. This feature also allows you to specify the percentage of bandwidth to be allocated to nonpriority traffic classes.

This feature modifies two existing commands—**bandwidth** and **priority**. This feature adds a new keyword to the **bandwidth** command—**remaining percent**. The feature also changes the functionality of the existing **percent** keyword. These changes result in the following commands for bandwidth: **bandwidth percent** and **bandwidth remaining percent**. The **bandwidth percent** command configures bandwidth as an absolute percentage of the total bandwidth on the interface. The **bandwidth remaining percent** command allows you to allocate bandwidth as a relative percentage of the total bandwidth available on the interface. This command allows you to specify the relative percentage of the bandwidth to be allocated to the classes of traffic.

This feature also adds the **percent** keyword to the **priority** command. The **priority percent** command indicates that the bandwidth will be allocated as a percentage of the total bandwidth of the interface. You can then specify the percentage (that is, a number from 1 to 100) to be allocated by using the *percentage* argument with the **priority percent** command.

Unlike the **bandwidth** command, the **priority** command provides a strict priority to the traffic class, which ensures low latency to high priority traffic classes. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftllqpct.htm.

Note This feature was originally introduced in Cisco IOS Release 12.0(5)T. This release adds the **remaining percent** keyword.

MGCP CAS PBX and PRI Backhaul on Cisco 7200 Series Routers

The MGCP CAS PBX and PRI Backhaul on Cisco 7200 Series Routers features extend the earlier Simple Gateway Control Protocol (SGCP) channel-associated signaling (CAS) and AAL2 support onto the merged SGCP/MGCP software base to enable various service provider solutions.

PRI/Q.931 Signaling Backhaul is the ability to reliably transport the signaling (Q.931 and above layers) from a PRI trunk that is physically connected to a media gateway (for example, a Cisco 7200 series router) to a media gateway controller (Cisco VSC3000) for processing.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft_mg7xx.htm

MGCP CAS PBX and AAL2 PVC with Basic CLASS and Operator Services

The MGCP CAS PBX and AAL2 PVC software package is a solutions-oriented program that focuses on several customer gateway scenarios. These scenarios require features that address residential, business, and trunking gateway needs on a variety of hardware platforms:

- Residential cable connectivity
- CAS and analog PBX connectivity
- Incoming CAS support for trunking gateways that support operator services such as busy-line verify and barge-in xGCP support of Voice over ATM Adaption Layer type 2 (VoAAL2)

To answer these needs, the MGCP CAS PBX and AAL2 PVC feature combines and expands existing feature sets on the merged Simple Gateway Control Protocol (SGCP)/MGCP software platform as follows:

- Voice over IP (VoIP) support of selected channel-associated signaling (CAS) features
- SGCP AAL2 features

Refer to the following documents for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcptk.htm.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcpgr.htm.

MGCP VoIP Signaling for 1750 Series

The MGCP CAS PBX and AAL2 PVC features extend the earlier Simple Gateway Control Protocol (SGCP) Channel Associated Signaling (CAS) and AAL2 support onto the merged SGCP/MGCP software base to enable various service provider solutions. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ftmgcpba.htm.

Mobile IP MIB Support for SNMP

The Mobile IP MIB Support for SNMP feature adds a MIB module that expands network monitoring capabilities of foreign agent (FA) and home agent (HA) mobile IP entities. Mobile IP management using SNMP is defined in two MIBs: the RFC2006-MIB and the CISCO-MOBILE-IP-MIB. The Cisco Mobile IP MIB is a Cisco enterprise-specific extension to IETF RFC 2006 MIB module that allows you to monitor the total number of HA Mobile bindings and the total number of FA visitor bindings. Cisco IOS Release 12.2(2)T also adds support for RFC 2006 Set operations and a SNMP notification. Set operations (performed from a Network Management System) are supported for starting and stopping the mobile IP service, configuring security associations, modifying advertisement parameters, and configuring "care-of addresses" for foreign agents. An SNMP notification (trap or inform) for security violations can be enabled on supported routing devices using the **snmp-server enable traps ipmobile** and **snmp-server host** global configuration CLI commands. Because this feature affects security, use of SNMPv3 is strongly recommended.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft1mip.htm.

Modem Script and System Script Support in Large-Scale Dial-Out

Modem connection and system login chat scripts are often used when asynchronous dial-on-demand routing (DDR) is configured. Currently, however, the large-scale dial-out network architecture does not allow chat scripts for a particular session to be passed through the network. Cisco IOS Release 12.2(2)T allows modem and system chat scripts to pass through large-scale dial-out networks by allocating two new authentication, authorization, and accounting (AAA) attributes for outbound service.

The AAA attributes define specific AAA elements in a user profile. Large-scale dial-out supports Cisco attribute-value (AV) pairs and TACACS+ attributes. The Modem Script and System Script Support in Large-Scale Dial-Out feature provides two new outbound service attributes for passing chat scripts: modem-script and system-script.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftlschat.htm.

MPLS Label Distribution Protocol

The Cisco MPLS label distribution protocol (LDP) allows the construction of highly scalable and flexible IP Virtual Private Networks (VPNs) that support multiple levels of services.

LDP provides a standard methodology for hop-by-hop distribution of labels in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting label switch paths (LSPs) forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement the Cisco MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

LDP enables label switching routers (LSRs) to request, distribute, and release label prefix binding information to peer routers in a network. Thus, LSRs can discover potential peers and establish LDP sessions with those peers to exchange label binding information.

LDP is a superset of the Cisco prestandard Tag Distribution Protocol (TDP), which also supports MPLS forwarding along normally routed paths. For the features that LDP and TDP share in common, the pattern of protocol exchange between network routing platforms is identical. The differences between LDP and TDP for those features supported by both protocols are largely embedded in their respective implementation details, such as the encoding of protocol messages.

This release of LDP supports both the LDP and TDP protocols and provides the means for changing an existing network from a TDP environment to an LDP environment. Thus, you can run LDP and TDP simultaneously on any router platform. The routing protocol that you select can be configured on a per-interface basis for directly connected neighbors and on a per-session basis for nondirectly connected (targeted) neighbors. In addition, an LSP across an MPLS network can be supported by LDP on some hops and by TDP on other hops.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ldp_221t.htm.

MPLS Label Distribution Protocol MIB

The MPLS label distribution protocol (LDP) MIB is an idealized label switching database that provides an effective management infrastructure for using LDP in an MPLS network.

The notation used in the MPLS LDP MIB adheres to the conventions defined in the Abstract System Notation One (ASN.1) standard, which defines an Open System Interconnection (OSI) language used in describing data types independently from particular computer structures and presentation techniques.

Each object in the MPLS LDP MIB incorporates a DESCRIPTION field that describes the meaning and usage of the object, which, together with other object characteristics, provides information that enables network administrators to monitor and control network devices, measure network performance, and collect network statistics.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ldpmib2t.htm.

MPLS Label Switching Router MIB

The MPLS Label Switching Router MIB allows you to use the Simple Network Management Protocol (SNMP) to remotely monitor a label switching router (LSR) that is using the Multiprotocol Label Switching (MPLS) technology. The MPLS-LSR-MIB mirrors the Cisco Label Switching subsystem, specifically the LSR management information that is provided by the label forwarding information base (LFIB).

The MPLS-LSR-MIB contains managed objects that support the retrieval of label switching information from a router and is based on Revision 05 of the IEFT MPLS-LSR-MIB. This implementation enables a network administrator to get information on the status, character, and performance of the following:

- MPLS capable interfaces on the LSR
- Incoming MPLS segments (labels) to an LSR and their associated parameters
- Outgoing segments (labels) from an LSR and their associated parameters

In addition, the network manager can retrieve the status of cross-connect entries that associate MPLS segments together. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/lsrmibt.htm.

MPLS QoS Multi-VC Mode for PA-A3

MPLS QoS Multi-VC Mode functionality substantially enhances MPLS quality of service (QoS) capabilities. This new MPLS QoS feature enables users to map the experimental (EXP) field value of an MPLS label to an ATM virtual circuit (VC) to create "bundles" of labeled virtual circuits (LVCs). Each bundle consists of multiple LVCs, and each LVC is treated as a member of the bundle.

Each member of a bundle can be associated with any pair of ATM-connected routers in the networking environment of the user, and each member of a bundle can have a QoS different from other members of the bundle.

By means of virtual circuit bundles, differentiated services can be provided to users of MPLS-enabled service provider networks. This service differentiation is accomplished by setting an appropriate value in the EXP field in the header of each incoming packet as it is received by the provider edge (PE) router in the service provider network.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/cos1221t.htm.

MPLS Traffic Engineering MIB

SNMP agent code operating in conjunction with the MPLS TE MIB enables a standardized, SNMP-based approach to be used in managing the MPLS traffic engineering features in Cisco IOS software.

The MPLS TE MIB is based on the IETF draft MIB entitled draft-ietf-mpls-te-mib-05.txt, which includes objects describing features that support MPLS traffic engineering. This IETF draft MIB, which undergoes revisions from time to time, is being evolved toward becoming a standard. Accordingly, the Cisco implementation of the MPLS TE MIB is expected to track the evolution of the IETF draft MIB.

Slight differences between the IETF draft MIB and the implementation of the traffic engineering capabilities within Cisco IOS software require some minor translations between the MPLS TE MIB and the internal data structures of Cisco IOS software. These translations are accomplished by means of the SNMP agent code that is installed and operating on various hosts within the network. This SNMP agent code, running in the background as a low priority process, provides a management interface to Cisco IOS software.

The SNMP objects defined in the MPLS TE MIB can be displayed using any standard SNMP utility. All MPLS TE MIB objects are based on the IETF draft MI, which means that no specific Cisco SNMP application is required to support the functions and operations pertaining to the MPLS TE MIB.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/te_mib12.htm.

NAT Support of H.323 RAS

The Cisco IOS NAT feature supports all H.225 and H.245 message types, including Registration, Admission, and Status (RAS). RAS provides a number of messages that are used by software clients and VoIP devices to register their location, request assistance in call setup, and control bandwidth. The RAS messages are directed toward an H.323 gatekeeper.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftnatras.htm.

NetFlow Multiple Export Destinations

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to the destination host. Currently, the maximum number of export destinations allowed is two.

The NetFlow Multiple Export Destinations feature improves the chances of receiving complete NetFlow data by providing redundant streams of data. Because the same export data is sent to more than one NetFlow collector, fewer packets will be lost.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/dtnfdest.htm.

Network-Based Application Recognition

Network-Based Application Recognition is now supported on Cisco 1700 series routers.

As IP quality of service (QoS) technology matures and customers begin QoS deployment in production networks, new requirements for packet classification have emerged. The applications require high performance to ensure competitiveness in an increasingly fast-paced business environment. Networks provide a variety of services to ensure that mission-critical applications receive the required bandwidth for high performance. Internet-based and client/server applications make it difficult for networks to identify packets and provide the proper level of control.

Network-Based Application Recognition (NBAR) solves this level of control by adding intelligent network classification to network infrastructures. NBAR is a new classification engine that recognizes a wide variety of applications, including web-based and other difficult-to-classify protocols that utilize dynamic TCP/UDP port assignments. When an application is recognized and classified by NBAR, a network can invoke services for that specific application. NBAR ensures that network bandwidth is used efficiently by working with QoS features to provide the following features:

- Guaranteed bandwidth
- Bandwidth limits
- Traffic shaping
- Packet coloring

NBAR introduces several new classification features as follows:

- Classification of applications that dynamically assign TCP/UDP port numbers
- Classification of HTTP traffic by URL, host, or MIME type
- Classification of Citrix ICA traffic by application name
- Classification of application traffic using subport information

NBAR can also classify static port protocols. Although access control lists (ACLs) can also be used for this purpose, NBAR is easier to configure and can provide classification statistics that are not available when using ACLs.

NBAR provides a special Protocol Discovery feature that determines which application protocols are traversing a network at any given time. The Protocol Discovery feature captures key statistics associated with each protocol in a network. These statistics can be used to define traffic classes and QoS policies for each traffic class.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtnbar.htm.

PPP over Ethernet Client

The PPP over Ethernet Client feature provides PPP over Ethernet (PPPoE) client support on routers or digital subscriber line (DSL) modems on customer premises.

PPPoE client is supported on ATM permanent virtual circuits (PVCs) using a dialer interface for cloning virtual access. One PVC will support one PPPoE client. Multiple PPPoE clients can run concurrently on different PVCs, but each PPPoE client must use a separate dialer interface and a separate dialer pool.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftpppoec.htm.

Preauthentication with ISDN PRI and Channel-Associated Signaling Enhancements

Preauthentication allows a Cisco network access server (NAS) to decide—on the basis of the Dialed Number Identification Service (DNIS) number—whether to answer an incoming call. When an incoming call arrives from the public network switch but before it is answered, the NAS sends the DNIS number to a RADIUS server for authorization.

The Preauthentication with ISDN PRI and Channel-Associated Signaling Enhancements feature provides additional support for preauthentication, which was introduced in a previous Cisco IOS release. For more information about preauthentication, refer to the Cisco IOS Release 12.1(3)T feature module titled *Preauthentication with ISDN PRI and Channel-Associated Signaling*.

This feature supports the use of attribute 44 by the RADIUS server application, which allows user authentication on the basis of the Calling Line Identification (CLID) number in the same transaction. For more information about attribute 44 and how it works with preauthentication, refer to the Cisco IOS Release 12.0(7)T feature module titled *RADIUS Attribute 44 (Accounting Session ID) in Access Requests*.

This feature also supports the use of new RADIUS attributes. These RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdtl.htm.

Prefix Dial for 800 Series Routers

Cisco 803 and Cisco 804 routers now support prefix dialing. You can add a telephone prefix and create a prefix filter to the dialed number for analog telephone calls. When a telephone number is dialed through the telephone port, the router checks for prefix filters. If the router finds a match, no prefix is added to the dialed number. If no filter match is found, the router adds the user-defined prefix to the called number.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft_vs800.htm.

Quality of Service for Virtual Private Networks

When packets are encapsulated by tunnel or encryption headers, Quality of Service (QoS) features are unable to examine the original packet headers and correctly classify the packets. Packets traveling across the same tunnel have the same tunnel headers, so the packets are treated identically if the physical interface is congested.

With the growing popularity of Virtual Private Networks (VPNs), the need to classify traffic within a traffic tunnel is gaining importance. QoS features have historically been unable to classify traffic within a tunnel. With the introduction of the Quality of Service for Virtual Private Networks (QoS for VPNs) feature, packets can now be classified before tunneling and encryption occur. The process of classifying features before tunneling and encryption is called preclassification.

The QoS for VPNs feature is designed for tunnel interfaces. When the new feature is enabled, the QoS features on the output interface classify packets before encryption, allowing traffic flows to be adjusted in congested environments. The end result is more effective packet tunneling.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtqosvpn.htm.

RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements

Virtual private networks (VPNs) use Layer 2 Forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP) tunnels to tunnel the link layer of high-level protocols (for example, PPP) or asynchronous High-Level Data Link Control (HDLC)). Internet service providers (ISPs) configure their network access servers (NASs) to receive calls from users and forward the calls to the customer tunnel server. Usually, the ISP maintains only information about the tunnel server—the tunnel endpoint. The customer maintains the IP addresses, routing, and other user database functions of the tunnel server users.

The RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature adds the ability to specify the host name of the NAS—rather than the IP address of the NAS—in RADIUS attribute 66 (Tunnel-Client-Endpoint).

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdt4.htm.

RSVP Scalability Enhancements

RSVP typically performs admission control, classification, policing, and scheduling of data packets on a per-flow basis and keeps a database of information for each flow. RSVP scalability enhancements let you select a resource provider (formerly called a quality of service (QoS) provider) and disable data-packet classification so that RSVP performs admission control only. These enhancements facilitate integration with service provider (differentiated services) networks and enables scalability across enterprise networks.

Class-based weighted fair queueing (CBWFQ) provides the classification, policing, and scheduling functions. CBWFQ puts packets into classes based on the differentiated services code point (DSCP) value in the IP header of the packet, thereby eliminating the need for per-flow state and per-flow processing.

There are two new commands:

ip rsvp data-packed classifications none—Disables data packet classification.

ip rsvp resource-provider {*none* | *wfq interface* | *wfq pvc*}—Configures a resource provider for an aggregate flow.

There is one modified command:

show ip rsvp interface detail—The detail keyword was added to display information about RSVP interface parameters.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/rsvpscal.htm

RSVP Support for ATM/PVCs

The RSVP Support for ATM/PVCs feature allows RSVP to function with per-PVC queueing for voice-like flows. Specifically, RSVP can install reservations on PVCs defined at the interface and subinterface levels. There is no limit to the number of PVCs that can be configured per interface or subinterface.

There are two new commands:

ip rsvp layer2 overhead [*h c n*]—Controls the overhead accounting performed by RSVP/WFQ when a flow is admitted onto an ATM PVC.

ip rsvp resource-provider {*none* | *wfq interface* | *wfq pvc*}—Configures a resource provider for an aggregate flow.

There is one modified command:

show ip rsvp interface detail—The detail keyword was added to display information about RSVP interface parameters.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/rsvp_atm.htm.

SA Agent Support for Application Monitoring, Frame Relay, VoIP, and MPLS VPN

The Cisco Service Assurance Agent (SA Agent) is a Cisco IOS software network monitoring solution. This enhancement to the Cisco SA Agent provides the following features: Application Performance Monitoring, Frame Relay Monitoring, Path Jitter, and MPLS VPN awareness.

SA Agent Application Performance Monitor (APM) operations allow the user to monitor performance of applications over a network. Monitoring the performance of network-hosted applications gives service providers and IT departments the ability to verify that applications are performing as needed and to implement improvements as necessary.

SA Agent Frame Relay Monitor (FRM) operations allow the user to monitor key performance metrics (round trip latency, packet loss, and data integrity) over Frame Relay PVCs. Proactively monitoring the performance of Frame Relay networks is essential for service providers that offer Frame Relay services.

SA Agent path echo operations have been enhanced to provide hop-by-hop jitter measurement using ICMP packets for VoIP monitoring. The Cisco SA Agent has also been enhanced to allow monitoring within MPLS Virtual Private Networks (VPNs).

Refer to the following document for additional information about the SA Agent Application Performance Monitor:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft2_apm.htm.

Refer to the following document for additional information about the SA Agent Support for Frame Relay, VoIP, and MPLS VPN Monitoring:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft1csaa.htm.

Secure Copy

The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that it is reliant upon SSH for security. In addition, SCP requires that AAA authorization be configured so the router can determine whether the user has the correct privilege level.

SCP allows a user logged in to Cisco IOS software to copy anything that exists in the Cisco IOS File System (IFS) to and from a router by using the **copy** command. A user using a remote workstation cannot perform this task.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftscp.htm.

Secure Shell Terminal-Line Access

Although Cisco IOS supports reverse Telnet, which allows users to Telnet to a certain port range that connects them to tty (asynchronous) lines, Telnet provides no security because all Telnet traffic goes over the network in the clear. The SSH Terminal-Line Access feature replaces reverse Telnet with secure shell (SSH), thereby, allowing users to configure their Cisco IOS routers securely.

The SSH Terminal-Line Access feature enables users to configure their router with secure access and perform the following tasks:

- Connect to a router that has multiple terminal lines connected to consoles of other routers.
- Simplify connectivity to a router from anywhere by securely connecting to the terminal server on a specific line.
- Allow modems attached to routers to be used for dial-out securely.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftrevssh.htm.

Shell-Based Authentication of VPDN Users

The Shell-Based Authentication of VPDN Users feature provides terminal services for VPDN users to support rollout of wholesale dial networks. Terminal services (shell login or exec login) on the network access server (NAS) provide the following capabilities:

- Enabling a dial-in user session to be terminated at the access server.
- Authenticating the user with a character-mode login dialog such as username/password or username/challenge/password, Secure ID, Safeword, and so on.
- Initiating PPP and tunneling it to a home gateway (HGW).

With the terminal services, user authentication methods other than PAP and CHAP can be applied to PPP users. With the Shell-Based Authentication of VPDN Users feature, PPP authentication data is preconfigured or entered before PPP starts. Authentication is completed without any further input from the user.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftexvpnt.htm.

SIP Diversion Header Implementation for Redirecting Number

SIP is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to the ITU-T H.323 specification. SIP is defined by RFC 2543 and is used for multimedia call session setup and control over IP networks. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/sipcf2.htm.

SIP Gateway Support for Third-Party Call Control

SIP is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to the ITU-T H.323 specification. SIP is defined by RFC 2543 and is used for multimedia call session setup and control over IP networks. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/sipcf2.htm.

SLT Dual Ethernet

The Cisco SLT Dual Ethernet feature adds Cisco SLT dual Ethernet support to the virtual switch controller (VSC). This enhanced Cisco SLT support provides two IP networks and two additional Session Manager sessions (for a total of four Session Manager sessions) for improved backhaul communication. These additions increase the resilience of Cisco SLT/VSC communications by supporting two RUDP sessions from each Ethernet interface to each VSC. These VSC enhancements contribute to determining when to switch Ethernets and when to switch VSC activity.

The Cisco SLT, which is based on the Cisco 2611 Multi-Service Access Router, is shipped with two Ethernet interfaces. Until this feature was released, the Cisco SLT/VSC solution supported only one of the two Ethernet interfaces. Both Session Manager sessions needed to travel over this single Ethernet interface: This Ethernet was a single-point failure. The Cisco SLT Dual Ethernet feature supports the second Ethernet, which improves the resilience of the backhaul IP communications.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftsltdes.htm.

SLT G.732 Support

The Cisco SLT enables service providers to reliably transport Signaling System 7 (SS7) protocols across an IP network. The Cisco SLT uses the Cisco IOS SS7 SLT feature set, providing reliable interoperability with the Cisco SC2200 or the Cisco VSC3000 device. The Cisco SLT is responsible for terminating the Message Transfer Part (MTP) 1 and MTP 2 layers of the SS7 protocol stack. Using the Cisco Reliable User Datagram Protocol (RUDP), the Cisco SLT backhauls, or transports, upper-layer SS7 protocols across an IP network to the Cisco SC2200 or VSC3000 device. The Cisco SLT is supported only on the Cisco 2611 router.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft_g732.htm.

SNMP Support over VPN

The SNMP Support over VPN feature allows the sending and receiving of SNMP notifications using VPN Routing Forwarding table (VRF).

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents.

A VPN is a network that provides high connectivity transfers on a shared system with the same usage guidelines as a private network. A VPN can be built on the Internet or on the service provider IP, Frame Relay, or ATM system.

A VRF stores per-VPN routing data. It defines the VPN membership of a customer site attached to the network access server (NAS). A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, guidelines, and routing protocol parameters that control the information that is included in the routing table.

The SNMP Support over VPN feature provides configuration commands that allow users to associate SNMP agents and managers with specific VRFs. The specified VRF is used for the sending of SNMP notifications (traps and informs) and responses between agents and managers. If a VRF is not specified, the default routing table for the VPN is used.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftnm_vpn.htm

SNMP Trap Support for the Virtual Switch Interface Master MIB

The VSI Master MIB allows you to manage and monitor the activities of the VSI components, including controllers, sessions, logical interfaces, and cross-connects. The MIB provides notifications in the form of traps when any of the VSI components change operational state, violate configured thresholds, or are added or removed.

The MIB allows you to specify which VSI components can send traps. To enable the traps for certain VSI components, you can use the MIB objects or Cisco IOS commands.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/mstrmib.htm.

Supplementary Telephone Services for the Euro-ISDN Switch

The Cisco 800 series routers now support the following plain old telephone service (POTS) features for the European Telecommunications Standards Institute (ETSI) Euro-ISDN switch type:

- Caller ID presentation and restriction are available for Denmark, Finland, and Sweden.
- Calling line identification restriction (CLIR) temporarily prevents your calling ID from being presented to the destination number for an outgoing call. You must configure CLIR prior to each call in which you want to restrict the calling party number from being presented at the destination.
- Call forwarding is enabled using Cisco IOS and dual tone multifrequency (DTMF) keypad commands.
- Call transfer enables you to connect two call destinations. The request for this service must originate from an active, outgoing call.

Note The Euro-ISDN switch was previously called the NET3 switch.

- The following types of voice call forwarding services are supported on the Euro-ISDN switch:
  - Call forward unconditional (CFU) redirects your calls without restrictions and takes precedence over other call forwarding types.
  - Call forward busy (CFB) redirects your call to another number if your number is busy.
  - Call forward no reply (CFNR) forwards your call to another number if your number does not answer within a specified period of time.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft_vs800.htm.

TCL IVR disconnect cause-code Manipulation

The **leg disconnect** command disconnects one or more call legs that are not part of any connection. The *cause_code* argument, which has been added in Cisco IOS Release 12.2(1)T, is an integer ISDN cause code for the disconnect. It is of the form di-*xxx* or just *xxx*, where *xxx* is the ISDN cause code. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2.htm.

Traffic Policing

The Traffic Policing feature performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria.
- Marks packets by setting the ATM Cell Loss Priority (CLP) bit, Frame Relay Discard Eligibility (DE) bit, IP precedence value, IP differentiated services code point (DSCP) value, MPLS experimental value, and Quality of Service (QoS) group.

Traffic policing allows you to control the maximum rate of traffic transmitted or received on an interface. The Traffic Policing feature is applied when you attach a traffic policy contain the Traffic Policing configuration to an interface. A traffic policy is configured using the Modular Quality of Service Command-Line Interface (Modular QoS CLI).

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftpoli.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(5)T. This release adds the set-clp-transmit, set-frde-transmit, and set-mpls-exp-transmit options for the *action* argument to the **police** command.

Trimble Palisade NTP Synchronization Driver for the Cisco 7200 Series Routers

The Trimble Palisade Smart Antenna can provide a signal that can by used for NTP time-synchronization of a network. The Trimble Palisade NTP Synchronization Kit can be connected to the auxiliary port of a Cisco 7200 router. The refclock (reference clock) driver provided by this feature provides the ability to receive an RTS time-stamp signal on the auxiliary port of the router.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t1/dtrimble.htm.

Using 31-bit Prefixes on IPv4 Point-to-Point Links

The Using 31-bit Prefixes on IPv4 Point-to-Point Links feature allows 31-bit prefixes to be used on IP version 4 point-to-point links. The number of IP addresses is reduced by 50 percent and the number of denial of service (DoS) attacks is also reduced. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft31addr.htm.

Voice over ATM with AAL2 Trunking on Cisco 7200 Series Routers

Voice over ATM (VoATM)

This feature enables Cisco 7200 series routers to carry voice traffic (for example, telephone calls and faxes) over ATM networks using AAL2. AAL2 is the most bandwidth-efficient standards-based trunking method for transporting compressed voice, voice-band data, circuit-mode data, and frame-mode data over ATM infrastructures.

Transparent Common Channel Signaling (T-CCS)

The Transparent Common Channel Signaling (T-CCS) feature provides a way to interconnect PBX, key systems (KTs), and central office (CO) switches when the private integrated services network exchange (PINX) does not support Q (point of the ISDN model) Signaling (QSIG), or when the PINX uses a proprietary solution. T-CCS allows the connection of two PBXs with PRI interfaces that use one CCS protocol without the need for interpretation of CCS signaling for call processing. A PBX PRI group is transported transparently through the data network, and the feature preserves proprietary signaling. From the PBX standpoint, this signaling is accomplished through a point-to-point connection. Calls from the PINXs are not routed, but follow a preconfigured route to the destination. Frame forwarding, used with T-CCS, forwards High-Level Data Link Control (HDLC) frames over a preconfigured interface running HDLC, Frame Relay, or ATM encapsulation.

Additional Information

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ft_aal72.htm.

X.25 Annex G Session Status Change Reporting

The X.25 Annex G Session Status Change Reporting feature introduces the **logging event frame-relay x25** interface configuration command, which provides console or system log notification of X.25 Annex G session status changes when an X.25 Annex G session carried over Frame Relay changes state. Before this feature was introduced, there was no notification.

This feature detects changes in session status using an X.25 Link Access Procedure, Balanced (LAPB) N2 counter. The LAPB N2 counter is the number of unsuccessful transmit attempts that are made before the link is declared down. After the N2 consecutive polled commands have not been answered, a notification is generated, indicating that the X.25 profile or context associated with the data-link connection identifier (DLCI) that is running across the failed radio link has gone down. A message is generated to the console or system log when the link goes down. A message is also generated to the console or system log when the link comes back up. The notification response time is contingent on the values assigned to the LAPB N1 counter and the LAPB T1 timer.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftanxg.htm.

MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 62.

Table 62 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2 T.

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/770/index.shtml. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/770/index.shtml.
- Product Bulletins—If you have an account on Cisco.com, you can find Product Bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find Product Bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.
- Deferral Advisories and Software Advisories for Cisco IOS Software—*Deferral Advisories and Software Advisories for Cisco IOS Software* provides information about caveats that are related to deferred software images for Cisco IOS releases. If you have an account on Cisco.com, you can access *Deferral Advisories and Software Advisories for Cisco IOS Software* at http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml.

- What's New for IOS—*What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml.
- Cisco IOS Software Roadmap—The *Cisco IOS Software Roadmap* illustrates the relationship of the various Cisco IOS releases. If you have an account on Cisco.com, you can access the *Cisco IOS Software Roadmap* at http://www.cisco.com/warp/customer/620/roadmap_b.shtml.

Important Notes for Cisco IOS Release 12.2(15)T4

The following information applies to Cisco IOS Release 12.2(15)T4.

Images Deferred Because of Caveats CSCea21186, CSCeb07534, CSCeb07595, and CSCeb10053

In Cisco IOS Release 12.2(15)T4, five images have been deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCea21186, CSCeb07534, CSCeb07595, and CSCeb10053. The affected images are as follows:

- rpm-boot-mz
- rpm-jk9o3s-mz
- rpm-js-mz
- rpmxf-boot-mz
- rpmxf-p12-mz

With caveat CSCea21186, TACACS server host command causes reload. With caveat CSCeb07534, reset of dual LSC in node-a results in tailend LVCs created on PE in node-b. With caveat CSCeb07595, provider edge (PE) box may reload after modifying MPLS partition VCIi range on an ATM interface. With caveat CSCeb10053, RPM runs out of buffers causing SAR no_buffer errors. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(15)T3

The following information applies to Cisco IOS Release 12.2(15)T3.

Images Deferred Because of Caveats CSCdx08292, CSCea57593, CSCea63209, CSCea67430, CSCea72272, CSCea73441, CSCea74222, CSCea75235, CSCea78687, CSCea84387, CSCea91135, CSCeb02097, and CSCeb02520

In Cisco IOS Release 12.2(15)T3, four images have been deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdx08292, CSCea57593, CSCea63209, CSCea67430, CSCea72272, CSCea73441, CSCea74222, CSCea75235, CSCea78687, CSCea84387, CSCea91135, CSCeb02097, and CSCeb02520. The affected images are as follows:

- rpm-boot-mz
- rpm-js-mz
- rpmxf-boot-mz
- rpmxf-p12-mz

With caveat CSCdx08292, auto-summary and sync not turned on by default under addr-fam VRF. With caveat CSCea57593, a Cisco RPM-PR router may reload with a bus error at 0x600ED128. With caveat CSCea63209, with dual LSCs and 1:N redundancy configured, one might experience a 10+ sec data disruption when a resetcd is issued for the active/primary LSC. With caveat CSCea67430, SNMP MIB variables are accessible to VRF interfaces on the RPM. With caveat CSCea72272, configuration file goes corrupt with multiple simultaneous VTY write memory. With caveat CSCea73441, RPM Path-Check causes router reset. With caveat CSCea74222, IGP label rewrite information for remote PE is lost from CEF table on a local PE. With caveat CSCea75235, during LSC switchover, a second outage found. With caveat CSCea78687, LSNT: LDP goes up/down under congestion situation. With caveat CSVea84387, two simultaneous policy map displays cause problems. With caveat CSCea91135, RPM may stay in error state (auto recovery disabled/heartbeat going). With caveat CSCeb 02097, LSNT: saving configuration took long time. With caveat CSCeb02520, RPM-PR router configured as eLSR might reset upon execution of the **show queue** command where interface is of MPLS type. The software solution for these deferred images is Cisco IOS Release 12.2(15)T5.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(15)T1

The following information applies to Cisco IOS Release 12.2(15)T1.

Images Deferred Because of Caveat CSCin40652

In Cisco IOS Release 12.2(15)T1, 352 images have been deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCin40652. The affected images are as follows:

• c820-k9osv6y6-mz	• c2691-io3-mz	• c3725-ix-mz	• c7200-jk9o3s-mz
• c820-k9osy6-mz	• c2691-is-mz	• c3725-jk9o3s-mz	• c7200-jk9s-mz
• c820-ov6y6-mz	• c2691-ix-mz	• c3725-jk9s-mz	• c7200-jo3s-mz
• c820-oy6-mz	• c2691-jk8o3s-mz	• c3725-jk9s2-mz	• c7200-js-mz
• c820-sv6y6-mz	• c2691-jk8s-mz	• c3725-js-mz	• c7200-jx2-mz
• c820-sy6-mz	• c2691-jk9o3s-mz	• c3725-js2-mz	• c7200-kboot-mz
• c820-v6y6-mz	• c2691-jk9s-mz	• c3725-jsx-mz	• c7200-p-mz
• c820-y6-mz	• c2691-js-mz	• c3725-p-mz	• c7400-a3jk8s-mz
• c1700-bk8no3r2sv3y7-mz	• c2691-jsx-mz	• c3745-a3jk9s-mz	• c7400-a3jk9s-mz
• c1700-bk8no3r2sv8y7-mz	• c2691-p-mz	• c3745-s3js-mz	• c7400-a3js-mz
• c1700-bk8no3r2sy7-mz	• c3620-i-mz	• c3745-bin-mz	• c7400-dk8o3s-mz
• c1700-bk9no3r2sv3y7-mz	• c3620-ik9o3s6-mz	• c3745-bino3s-mz	• c77400-dk8s-mz
• c1700-k9no3r2sv8y7-mz	• c3620-ik9o3s7-mz	• c3745-bins-mz	• c7400-dk9o3s-mz
• c1700-bk9no3r2sy7-mz	• c3620-in-mz	• c3745-i-mz	• c7400-do3s-mz
• c1700-bnr2sy7-mz	• c3620-ino3s3-mz	• c3745-ik9o3s-mz	• c7400-ds-mz
• c1700-bnr2y-mz	• c3620-io3-mz	• c3745-ik9s-mz	• c7400-g4js-mz
• c1700-k8o3sv3y7-mz	• c3620-is-mz	• c3745-io3-mz	• c7400-ik8o3s-mz
• c1700-k8o3sv8y7-mz	• c3620-is3x-mz	• c3745-is-mz	• c7400-ik8s-mz
• c1700-k8o3sy7-mz	• c3620-ix-mz	• c3745-ix-mz	• c7400-ik9o3s-mz
• c1700-k8sv3y7-mz	• c3620-jls3-mz	• c3745-jk9o3s-mz	• c7400-ik9s-mz
• c1700-k8sv8y7-mz	• c3631-telco-mz	• c3745-jk9s-mz	• c7400-io3s-mz
• c1700-k8sy7-mz	• c3631-telcoent-mz	• c3745-jk9s2-mz	• c7400-is-mz
• c1700-k9o3sv3y7-mz	• c3640-a3jk8s-mz	• c3745-js-mz	• c7400-jk8o3s-mz
• c1700-k9o3sv8y7-mz	• c3640-a3jk9s-mz	• c3745-js2-mz	• c7400-jk8s-mz
• c1700-k9o3sy7-mz	• c3640-a3js-mz	• c3745-jsx-mz	• c7400-jk9o3s-mz
• c1700-k9sv3y7-mz	• c3640-bin-mz	• c3745-p-mz	• c7400-jk9s-mz

c1700-k9sv8y7-mz	c3640-bino3s-mz	c4224-a3ik9no3rsx3-mz	c7400-jo3s-mz
c1700-k9sy7-mz	c3640-bins-mz	c4224-io3sx3-mz	c7400-js-mz
c1700-no3sv3y7-mz	c3640-i-mz	c4gwy-a3bik9no3rsx3-mz	c7400-jx2-mz
c1700-no3sv8y7-mz	c3640-ik8o3s-mz	c4gwy-binrsx3-mz	c7400-kboot-mz
c1700-no3sy7-mz	c3640-ik8s-mz	c4gwy-cboot-mz	c7400-p-mz
c1700-ny-mz	c3640-ik8sw6-mz	c4gwy-isx3-mz	cva120-k8boot-mz
c1700-o3sv3y7-mz	c3640-ik9o3s-mz	c5300-ik8s-mz	cva120-k8o3v9y5-mz
c1700-o3sv8y7-mz	c3640-ik9o3sw6-mz	c5300-ik9s-mz	ics7700-bk8no3r2sv3y-mz
c1700-o3y-mz	c3640-ik9s-mz	c5300-jk8s-mz	ics7700-bk9no3r2sv3y-mz
c1700-sv3y-mz	c3640-ik9sw6-mz	c5300-jk9s-mz	ics7700-bnr2sv3y-mz
c1700-sv3y7-mz	c3640-io3-mz	c5300-boot-mz	ics7700-k8o3sv3y-mz
c1700-sv8y-mz	c3640-is-mz	c5300-d-mz	ics7700-k9o3sv3y-mz
c1700-sv8y7-mz	c3640-ix-mz	c5300-ds-mz	ics7700-sv3y-mz
c1700-sy-mz	c3640-jk8o3s-mz	c5300-i-mz	mc3810-a2i5k8s-mz
c1700-sy7-mz	c3640-jk8s-mz	c5300-ik8s-mz	mc3810-a2i5k9s-mz
c1700-y-mz	c3640-jk9o3s-mz	c5300-is-mz	mx3810-a2i5s-mz
c1700-y7-mz	c3640-jk9s-mz	c5300-j-mz	mc3810-a2ik8sv5-mz
c2420-a2i8k8sv5-mz	c3640-js-mz	c5300-js-mz	mc3810-a2ik9s-mz
c2420-a2i8sv5-mz	c3640-jsx-mz	c5350-ik8s-mz	mc3810-a2ik9sv5-mz
c2600-a3jk8s-mz	c3640-k9p-mz	c5350-is-mz	mc3810-a2isv5-mz
c2600-a3jk9s-mz	c3640-p7-mz	c5350-jk8s-mz	mc3810-a2jk8sv5-mz
c2600-a3js-mz	c3640-telco-mz	c5350-js-mz	mc3810-a2jk9s-mz
c2600-bin-mz	c3660-a3jk8s-mz	c5400-boot-mz	mc3810-a2jk9sv5-mz
c2600-bino3s-mz	c3660-a3jk9s-mz	c5400-ik8s-mz	mc3810-a2jsv5-mz
c2600-bino3s3-mz	c3660-a3js-mz	c5400-is-mz	mc3810-a2jsv5x-mz
c2600-bins-mz	c3660-bin-mz	c5400-jk8s-mz	mc3810-i-mz
c2600-c-mz	c3660-bino3s-mz	c5400-js-mz	mc3810-i5k8s-mz
c2600-g4js-mz	c3660-bins-mz	c5800-k8p4-mz	mc3810-i5k9s-mz
c2600-i-mz	c3660-i-mz	c5800-p4-mz	mc3810-i5s-mz
c2600-ik8o3s-mz	c3660-ik8o3s-mz	c5850-boot-mz	mc3810-ik8s-mz
c2600-ik8s-mz	c3660-ik8s-mz	c5850-k8p9-mz	mc3810-ik9s-mz
c2600-ik9o3s-mz	c3660-ik8sw6-mz	c5850-k9p9-mz	mc3810-is-mz
c2600-ik9o3s3-mz	c3660-ik9o3s-mz	c5850-p9-mz	mc3810-jk8s-mz
c2600-ik9s-mz	c3660-ik9o3sw6-mz	c7100-ik8o3s-mz	mc3810-jk9s-mz

- c2600-io3-mz
- c2600-ipss7-mz
- c2600-is-mz
- c2600-is3x-mz
- c2600-is4-mz
- c2600-is5-mz
- c2600-ix-mz
- c2600-jls3-mz
- c2600-jk8o3s-mz
- c2600-jk8s-mz
- c2600-jk9o3s-mz
- c2600-jk9s-mz
- c2600-jk9s2-mz
- c2600-js-mz
- c2600-js2-mz
- c2600-jsx-mz
- c2600-telco-mz
- c2691-a3jk8s-mz
- c2691-a3jk9s-mz
- c2691-a3js-mz
- c2691-bin-mz
- c2691-bino3s-mz
- c2691-bins-mz
- c2691-i-mz
- c2691-ik8o3s-mz
- c2691-ik8s-mz
- c2691-ik9o3s-mz
- c2691-ik9s-mz
- c3660-ik9s-mz
- c3660-ik9sw6-mz
- c3660-io3-mz
- c3660-is-mz
- c3660-ix-mz
- c3660-jk8o3s-mz
- c3660-jk8s-mz
- c3660-jk9o3s-mz
- c3660-jk9s-mz
- c3660-jk9s2-mz
- c3660-js-mz
- c3660-js2-mz
- c3660-jsx-mz
- c3660-k9p-mz
- c3660-p-mz
- c3660-telco-mz
- c3660-telcoent-mz
- c3660-telcoentk9-mz
- c3725-a3jk9s-mz
- c3725-a3js-mz
- c3725-bin-mz
- c3725-bino3s-mz
- c3725-bins-mz
- c3725-i-mz
- c3725-ik9o3s-mz
- c3725-ik9s-mz
- c3725-io3-mz
- c3725-is-mz
- c7100-ik8s-mz
- c7100-ik9o3s-mz
- c7100-ik9s-mz
- c7100-io3s-mz
- c7100-is-mz
- c7100-jk8o3s-mz
- c7100-jk8s-mz
- c7100-jk9o3s-mz
- c7100-jk9s-mz
- c7100-jo3s-mz
- c7100-js-mz
- c7100-p-mz
- c7200-a3jk8s-mz
- c7200-a3jk9s-mz
- c7200-a3js-mz
- c7200-dk8o3s-mz
- c7200-dk8s-mz
- c7200-dk9o3s-mz
- c7200-do3s-mz
- c7200-ds-mz
- c7200-g4js-mz
- c7200-ik8o3s-mz
- c7200-ik8s
- c7200-ik9o3s-mz
- c7200-ik9s-mz
- c7200-io3s-mz
- c7200-is-mz
- c7200-jk8o3s-mz
- c7200-jk8s-mz
- mc3810-js-mz
- rsp-a3jk8sv-mz
- rsp-a3jk9sv-mz
- rsp-a3jsv-mz
- rsp-boot-mz
- rsp-dk8o3sv-mz
- rsp-dk8sv-mz
- rsp-dk9o3sv-mz
- rsp-do3sv-mz
- rsp-dsv-mz
- rsp-ik8o3sv-mz
- rsp-ik8sv-mz
- rsp-ik9o3sv-mz
- rsp-ik9sv-mz
- rsp-io3sv-mz
- rsp-isv-mz
- rsp-jk8o3sv-mz
- rsp-jk8sv-mz
- rsp-jk9o3sv-mz
- rsp-jk9sv-mz
- rsp-jo3sv-mz
- rsp-jsv-mz
- rsp-p-mz
- rsp-pv-mz
- ubr925-k9o3sv9y5-mz
- urm-is-mz
- urm-jk9s-mz
- urm-js-mz
- vg200-i6s-mz

With caveat CSCin40652, Media Gateway Control Protocol (MGCP) channel-associated signaling (CAS) does not recieve path confirmation from terminating gateway. The software solution for these deferred images is Cisco IOS Release 12.2(15)T2.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(15)T

The following information applies to Cisco IOS Release 12.2(15)T.

Cisco Images Deferred Because of Caveats CSCdv82735, CSCea08727, CSCea11340, CSCea17465, CSCea35454, and CSCin38050

Six images in Cisco IOS Release 12.2(15)T were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdv82735, CSCea08727, CSCea11340, CSCea17465, CSCea35454, and CSCin38050. These caveats affect the following images:

- c4224-a3ik9no3rsx3-mz
- c4224-io3sx3-mz
- c2500-is-l
- c2600-g4js-mz
- ubr925-k9o3sv9y5-mz
- ubr925-k9o3sy5mz

With caveat CSCdv82735, speed/duplex cannot be hard set on FE ports connected to IP phone. With caveat CSCea08727, local-address broken in Cisco Easy VPN configuration. With caveat CSCea11340, Cisco Easy VPN web interface is broken on Cisco uBR925. With caveat CSCea17465, input queue size may go negative leading to the Cisco Easy VPN connections getting stuck on the Cisco uBR925. With caveat CSCea35454, the c2500-is-l image size is too large for maximum memory. With CSCin38050, there is wrong accounting for PPPoX SSG users. The software solution for these deferred images is Cisco IOS Release 12.2(15)T1.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(13)T1

The following information applies to Cisco IOS Release 12.2(13)T1.

Cisco 1600 Series Router Images Deferred Because of Caveat CSCdz38371

Two images in Cisco IOS Release 12.2(13)T1 were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdz38371. This caveat affects the following images:

- c1600-bk8nor2sy-1
- c1600-bk8nor2sy-mz

With caveat CSCdz38371, the c1600-bk8nor2sy-1 and c1600-bk8nor2sy-mz images are too large for maximum router flash. The software solution for these deferred images is Cisco IOS Release 12.2(11)T3.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(13)T

The following information applies to Cisco IOS Release 12.2(13)T.

Cisco 1600 Series Router Images Deferred Because of Caveat CSCdz38371

Two images in Cisco IOS Release 12.2(13)T were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdz38371. This caveat affects the following images:

- c1600-bk8nor2sy-1
- c1600-bk8nor2sy-mz

With caveat CSCdz38371, the c1600-bk8nor2sy-1 and c1600-bk8nor2sy-mz images are too large for maximum router flash. The software solution for these deferred images is Cisco IOS Release 12.2(11)T3.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Cisco 3620 Series Router Images Deferred Because of Caveat CSCdz45923

Two images in Cisco IOS Release 12.2(13)T were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdz45923. This caveat affects the following images:

- c3620-bin-mz
- c3620-bino3s3-mz

With caveat CSCdz45923, Appletalk is missing from Cisco 3620 images. The software solution for this deferred image is Cisco IOS Release 12.2(15)T.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Cisco AS5800 Images Deferred Because of Caveats CSCdz04856, CSCdz09639, CSCdz26779, and CSCdy87529

Three images in Cisco IOS Release 12.2(13)T were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdz04856, CSCdz09639, CSCdz26779, and CSCdy87529. These caveats affect the following images:

- c5800-k8p4-mz
- dsc-c5800-mz
- c5800-p4-mz

With caveat CSCdz04856, a Cisco UPC324 dial feature card may stop accepting analog calls after running for about two hours. With caveat CSCdz09639, RS reloads at rs_set_debounce_timer after sh run.With caveat CSCdz26779, CRM shows resource active even after calls are disconnected. With caveat CSCdy87529, the Simple Network Management Protocol (SNMP) counters of a Cisco AS5800 may begin to deviate and may no longer reflect the actual number of calls when random analog and digital calls are received. The software solution for these deferred images is Cisco IOS Release 12.2(13)T1.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Cisco Catalyst 4000 Access Gateway Module Images Deferred Because of Caveat CSCdz27525

Cisco Catalyst 4000 Access Gateway Module images were deferred in Cisco IOS Release 12.2(13)T because of a severe defect. This defect has been assigned Cisco caveat ID CSCdz27525. This caveat affects the following images:

- c4gwy-a3ik9no3rsx3-mz
- c4gwy-a3ino3rsx3-mz
- c4gwy-io3sx3-mz

With caveat CSCdz27525, a Cisco Catalyst 4000 Gateway Module may experience a reload from overtemperature. The software solution for these deferred images is Cisco IOS Release 12.2(13)T2.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(11)T3

The following information applies to Cisco IOS Release 12.2(11)T3.

Cisco IAD2420 Images Deferred Because of Caveat CSCdz62759

Two images in Cisco IOS Release 12.2(11)T3 were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdz62759. This caveat affects the following images:

- c2420-a2i8sv5-mz
- c2420-a2i8k8sv5-mz

With caveat CSCdz62759, no ring-back tone when making hairpin calls between ports. The software solution for these deferred images is Cisco IOS Release 12.2(11)T4.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Important Notes for Cisco IOS Release 12.2(11)T2

The following information applies to Cisco IOS Release 12.2(11)T2.

Update to the mgcp fax t38 Command

Some Media Gateway Control Protocol (MGCP) call agents do not properly pass those portions of Session Description Protocol (SDP) messages that advertise T.38 and named service event (NSE) capabilities. As a result, gateways that are controlled by these call agents are unable to use NSEs to signal T.38 fax relay to other gateways that use NSEs. The new syntax for the **mgcp fax t38** command provides a way to enable gateway-controlled T.38 fax relay between an MGCP gateway and another gateway even if the capability to use T.38 and NSEs cannot be negotiated by the MGCP call agent at call setup time. The other gateway can be H.323, Session Initiation Protocol (SIP), or MGCP.

Important Notes for Cisco IOS Release 12.2(11)T

The following information applies to Cisco IOS Release 12.2(11)T.

Cisco Catalyst 4000 Access Gateway Module Images Deferred Because of Caveat CSCdy17203

Cisco Catalyst 4000 Access Gateway Module images were deferred in Cisco IOS Release 12.2(11)T because of a severe defect. This defect has been assigned Cisco caveat ID CSCdy17203. This caveat affects the following images:

- c4gwy-io3s-mz
- c4gwy-ik8o3s-mz
- c4gwy-ik9o3s-mz
- c4gwy-io3sx3-mz
- c4gwy-ik8o3sx3-mz
- c4gwy-ik9o3sx3-mz

With caveat CSCdy17203, a Cisco Catalyst 4000 Gateway Module may experience failure to reboot. The software solution for these deferred images is Cisco IOS Release 12.2(11)T1.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Cisco H.235 Accounting and Security Enhancements for Cisco Gateways

With the Cisco H.235 Accounting and Security Enhancements for Cisco Gateways feature, Cisco H.323 gateways support three levels of authentication:

- Endpoint—The Registration, Admission, and Status (RAS) channel used for gateway-to-gatekeeper signaling is not a secure channel. To ensure secure communication, H.235 allows gateways to include an authentication key in their RAS messages. This key is used by the gatekeeper to authenticate the source of the messages. At the endpoint level, validation is performed on all messages from the gateway. The cryptoTokens are validated using the password configured for the gateway.
- Per-Call—When the gateway receives a call over the telephony leg, it prompts the user for an account number and personal identification number (PIN). A separate authentication, authorization, and accounting (AAA) RADIUS server is needed for the accounting and authentication process. See *Prepaid Distributed Calling Card Via Packet Telephony* for more information. These two numbers are included in certain RAS messages sent from the endpoint and are used to authenticate the originator of the call.
- All—This option is a combination of the other two. With this option, the validation of cryptoTokens in automatic repeat request (ARQ) messages is based on an the account number and PIN of the user making a call and the validation of cryptoTokens sent in all the other RAS messages is based on the password configured for the gateway.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/ios_122/pul0242x.htm.

Note This feature was originally introduced in Cisco IOS Release 12.0(7)T on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 7200 series routers, and the Cisco MC3810, Cisco AS5300, and Cisco AS5800 platforms. This release is porting the feature into the Cisco AS5350 and Cisco AS5400 platforms.

Detecting Carrier Sense Errors on the Cisco uBR905 and Cisco uBR925 Cable Access Routers

The Cisco uBR905 and Cisco uBR925 cable access routers cannot detect carrier sense errors on the four Ethernet ports that connect the router to the subscriber's local area network. This is because the four Ethernet ports are provided by an internal hub that always provides a carrier sense signal to the Cisco IOS software, even if no Ethernet devices are connected to the external ports.

In particular, this means that the dot3StatsCarrierSenseErrors attribute in ETHERLIKE-MIB (RFC 2665) will never indicate any drops in carrier of the Ethernet interface.

Dialing Number Enhancement

The Dialing Number Enhancement feature removes previous restrictions on the number of dialed digits accepted as a valid telephone number in the Called Party number information element (IE) by an interface configured for the National or International numbering types.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftdilnme.htm

Displaying Alarm Settings on the Cisco AS5800

The **show vrm vdevices** command displays detailed information for digital signal processors (DSPs) or a brief summary for all voice feature cards (VFCs). The display provides information such as the following: the number of channels, channels per DSP, bitmap of digital signal processor modules (DSPMs), DSP alarm statistics, and version numbers. This information is useful in monitoring the current state of the VFCs on a Cisco AS5800 Universal Access Server. In Cisco IOS Release 12.2(11)T, the **alarms** keyword and *vfc-slot-number-for-alarms* argument have been added for the **show vrm vdevices** command.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_svv.htm.

Fine-Grain Address Segmentation in Dial Peers

The Fine-Grain Address Segmentation in Dial Peers feature applies to dial plans in universal gateways that use universal ports to handle simultaneous voice and modem calls. It enables you to indicate any numbers within the range that the peer normally handles that should be rejected because they go to modems.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/fx_dpsgw.htm.

Gatekeeper Alias Registration and Address Resolution Enhancements

The Gatekeeper Alias Registration and Address Resolution Enhancements feature allows you to configure multiple prefixes for a local zone and register an endpoint belonging to multiple zone prefixes. With this feature, gatekeepers can accept a registration request (RRQ) message that has multiple E.164 aliases that use different prefixes.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftgkar.htm.

MICA and NextPort Modem Tech-Support Commands for the AS5xxx Platforms

New **show tech-support** modem and **show tech-support spe** commands are useful to the Cisco customer and Cisco customer support personnel alike. For example, when quality assurance technicians gather troubleshooting information, rather than typing in a series of commands, the technicians can simply add the output of the **show tech-support** modem and **show tech-support spe** commands to their report. Development engineers can then have a consistent output to look at when troubleshooting problems.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftmodsho.htm.

OSP Client Performance Improvement

The **url** command change for the OSP Client Performance Improvement feature is a minor modification in the way that the settlement providers are configured. As a result of minimum command-line interface (CLI) change in the architecture, the Open Settlement Protocol (OSP) process must be shut down before any URL change is performed.

RADIUS Debug Enhancements

The RADIUS Debug Enhancements feature provides enhanced RADIUS output. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

The new feature provides enhanced RADIUS output display including the following:

- Packet dump in a more readable, user-friendly ASCII format than before
- Nontruncated display of attribute values
- Ability to select an abbreviated RADIUS **debug** output display

There is one modified command: **debug radius**—displays information associated with RADIUS in enhanced formats.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftdebug.htm.

SIP Media Inactivity Timer

The SIP Media Inactivity Timer feature enables Cisco gateways to monitor and disconnect Voice over IP (VoIP) calls if no Real-Time Control Protocol (RTCP) packets are received within a configurable time period.

When RTCP reports are not received by a Cisco gateway, the SIP Media Inactivity Timer feature releases the hung session and its network resources in an orderly manner. These network resources include the gateway digital signal processor (DSP) and time-division multiplexing (TDM) channel resources that are utilized by the hung sessions. Because call signaling is sent to tear down the call, any stateful Session Initiation Protocol (SIP) proxies involved in the call are also notified to clear the state that they have associated with the hung session. The call is also cleared back through the TDM port so that any attached TDM switching equipment also clears its resources.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftsiprtp.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

SS7 Interconnect to Lucent 1AESS Switches

The Lucent 1AESS local exchange telephone switching system was widely deployed in the 1970s across what was then the Bell System. During the past two decades, most 1AESS switches have been replaced by the next-generation digital switches, such as the Lucent 5ESS and Nortel DMS-100. While few 1AESSs remain, those still in service are generally heavily built out—about 2 to 5 percent of lines are on 1AESS switches.

Service providers that offer wholesale dial, Internet/intranet, and access Virtual Private Networks (VPNs) require remote access and expect to provide widely available service at the lowest cost. To do so, they must have Signaling System 7 (SS7) trunks to each local exchange in a service area. And for the Internet service provider (ISP) or competitive local exchange carrier (CLEC) that wants 100 percent dial coverage, interfacing to the remaining 1AESSs is mandatory.

Using SS7 signaling avoids investment in central office circuit switches, which must be used as concentration points for dial-in traffic to the access servers when ISDN PRI or in-band trunk signaling is used.

This feature provides 1AESS support for the Cisco AS5400. The configuration is on a T1 basis: one or several T1 lines are designated to support 1AESS, but no fractional T1s (FT1s) can be configured.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft1aessv.htm.

T1 CAS for VoIP

The T1 CAS for VoIP feature adds support for T1 channel-associated signaling (CAS) and limited support for E1 R2 signaling to the Cisco AS5800 and Cisco AS5850 with the Voice Feature Card (VFC).

CAS is the transmission of signaling information within the voice channel. Various types of CAS signaling are available in the T1 world. The most common forms of CAS signaling are loop-start, ground-start, and recEive and transMit (E&M). The biggest disadvantage of CAS signaling is its use of user bandwidth to perform signaling functions. CAS signaling is often referred to as robbed-bit-signaling because user bandwidth is being "robbed" by the network for other purposes. In addition to receiving and placing calls, CAS signaling also processes the receipt of Dialed Number Identification System (DNIS) and automatic number identification (ANI) information, which is used to support authentication and other functions.

T1 CAS capabilities have been implemented on the Cisco AS5800 and Cisco AS5850 VFC to enhance and integrate T1 CAS capabilities on common central office (CO) and PBX configurations for voice calls. The service provider application for T1 CAS includes connectivity to the public network using T1 CAS from the Cisco AS5800 or Cisco AS5850 to the end office switch. In this configuration, the Cisco AS5800 or Cisco AS5850 captures the dialed-number or called-party-number information and passes it along to the upper-level applications for interactive voice response (IVR) script selection, modem pooling, and other applications. Service providers also require access to calling party number, ANI, for user identification, for the billing account number, and in the future, for more complicated call routing.

Service providers who implement Voice over IP (VoIP) include traditional voice carriers, new voice and data carriers, and existing Internet service providers. Some of these service providers might use subscriber side lines for their VoIP connectivity to the Public Switched Telephone Network (PSTN); others will use tandem-type service provider connections.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/ios_122/ft_t1eas.htm.

Important Notes for Cisco IOS Release 12.2(8)T2

The following information applies to Cisco IOS Release 12.2(8)T2.

Use 12.2(8)T1 Version of c7200-kboot-mz Image

For Cisco IOS Release 12.2(8)T2, please use the c7200-kboot-mz image from Cisco IOS Release 12.2(8)T1. This image is available on Cisco.com.

Important Notes for Cisco IOS Release 12.2(8)T1

The following information applies to Cisco IOS Release 12.2(8)T1.

ATM OC-3 Network Modules

The ATM OC-3 Network Modules are not currently supported on the Cisco 2691, Cisco 3725, and Cisco 3745 platforms.

Cisco IGX 8400 Series URM Images Deferred Because of Caveat CSCdx41149

Three images in Cisco IOS Release 12.2(8)T1 were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdx41149. This caveat affects the following images:

- urm-is-mz
- urm-jk9s-mz
- urm-js-mz

With caveat CSCdx41149, a CiscoIGX84 series URM may experience an IPC failure. The software solution for these deferred images is Cisco IOS Release 12.2(8)T4.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Cisco 7200 Series Router Limitation

The maximum number of Modular QoS CLI (MQC) Quality of Service (QoS) policy maps on a Cisco 7200 series router is limited to 256.

Important Notes for Cisco IOS Release 12.2(8)T

The following information applies to Cisco IOS Release 12.2(8)T.

Changes to Feature Support with Cisco IOS Release 12.2(8)T

Starting with Cisco IOS Release 12.2(8)T, the following features are removed from all features and feature sets for the Cisco 2600 series, Cisco 3640, and Cisco 3660 platforms:

- LAN Extension
- Combinet Packet Protocol (CPP)
- HP Probe Protocol
- Exterior Gateway Protocol (EGP)
- IPX Netware Link State Protocol (NLSP)
- IPX Next Hop Routing Protocol (NHRP)
- XREMOTE
- Decnet Phase IV
- Banyan Virtual Integrated Network Service (VINES)
- Apollo Domain
- Xerox Network System (XNS)
- Wireless Point-to-Multipoint

Starting with Cisco IOS Release 12.2(8)T, the following features are removed or support is not included on all feature sets for the Cisco 3620:

- LAN Extension
- Combinet Packet Protocol (CPP)
- HP Probe Protocol
- Exterior Gateway Protocol (EGP)
- IPX Netware Link State Protocol (NLSP)
- IPX Next Hop Routing Protocol (NHRP)
- XREMOTE
- ATM LAN Emulation (LANE)
- Multiprotocol over ATM (MPOA)
- Decnet Phase IV
- Banyan Virtual Integrated Network Service (VINES)
- Apollo Domain
- Xerox Network System (XNS)
- Wireless Point-to-Multipoint
- Support for High Density Analog and Fax Network Modules (NM-HDA)

Starting with Cisco IOS Release 12.2(8)T, the following features were removed from all "IP Plus" images and incorporated into the "Enterprise Plus" images on the Cisco 2600 only:

- ATM LAN Emulation (LANE)
- Multiprotocol over ATM (MPOA)

Cisco IGX 8400 Series URM Images Deferred Because of Caveat CSCdx41149

Three images in Cisco IOS Release 12.2(8)T were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdx41149. This caveat affects the following images:

- urm-is-mz
- urm-jk9s-mz
- urm-js-mz

With caveat CSCdx41149, a CiscoIGX84 series URM may experience an IPC failure. The software solution for these deferred images is Cisco IOS Release 12.2(8)T4.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Enhanced Gigabit Ethernet Interface Processor Support on Cisco 7500/RSP Series

The Enhanced Gigabit Ethernet Interface Processor (GEIP+) is a single-port interface processor that, when combined with the appropriate optical fiber cable and a Gigabit Interface Converter (GBIC), provides one Gigabit Ethernet (GE) interface that is compliant with the IEEE 802.3z specification. The GE interface on aGEIP+ operates in full-duplex mode.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/vip1/vip4/10699dwg/index.htm.

HSRP Restructure

The output of the **show standby** command has been revised, making the output clearer and easier to use.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fthsrp.htm.

MPLS Defects in Cisco IOS Release 12.2(8)T

Because of the following caveats, it is recommended that you do not enable MPLS and/or Tag Switching on Cisco IOS Release 12.2(8)T. There are no workarounds. You can use the current version of the software release or wait until the next renumber build.

- CSCdw47263 (MPLS)
- CSCdw54940 (MPLS)
- CSCdw59938 (MPLS)
- CSCdw64740 (MPLS)
- CSCdw67208 (MPLS)
- CSCdw67882 (MPLS)
- CSCdw66983 (RPM)
- CSCdw69707 (RPM)

Feature module documentation for new MPLS features that appear in Cisco IOS Release 12.2(8)T are not supported due to the above-listed caveats.

Refer to the Field Notice at the following location for additional information:

http://www.cisco.com/warp/customer/770/fn18286.shtml.

SIP Media Inactivity Timer

The SIP Media Inactivity Timer feature enables Cisco gateways to monitor and disconnect Voice over IP (VoIP) calls if no Real-Time Control Protocol (RTCP) packets are received within a configurable time period.

When RTCP reports are not received by a Cisco gateway, the SIP Media Inactivity Timer feature releases the hung session and its network resources in an orderly manner. These network resources include the gateway digital signal processor (DSP) and time-division multiplexing (TDM) channel resources that are utilized by the hung sessions. Because call signaling is sent to tear down the call, any stateful Session Initiation Protocol (SIP) proxies involved in the call are also notified to clear the state that they have associated with the hung session. The call is also cleared back through the TDM port so that any attached TDM switching equipment also clears its resources.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftsiprtp.htm.

Important Notes for Cisco IOS Release 12.2(4)T

The following information applies to Cisco IOS Release 12.2(4)T.

Cisco 7500 Series Images Deferred Because of Caveat CSCdu01272

Twenty images in Cisco IOS Release 12.2(4)T were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCdu01272. This caveat affects the following images:

- rsp-a3jk8sv-mz
- rsp-a3jk9sv-mz

- rsp-a3jsv-mz
- rsp-dk8o3sv-mz
- rsp-dk8sv-mz
- rsp-dk9o3sv-mz
- rsp-do3sv-mz
- rsp-dsv-mz
- rsp-ik8o3sv-mz
- rsp-ik8sv-mz
- rsp-ik9o3sv-mz
- rsp-ik9sv-mz
- rsp-io3sv-mz
- rsp-isv-mz
- rsp-jk8o3sv-mz
- rsp-jk8sv-mz
- rsp-jk9o3sv-mz
- rsp-jk9sv-mz
- rsp-jo3sv-mz
- rsp-jsv-mz

With caveat CSCdu01272, a Cisco 7500 series with a PA-MC-T3 port adapter may experience a Versatile Interface Processor (VIP) reload. The software solution for these deferred images is Cisco IOS Release 12.2(2)T1, which is available on Cisco.com.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Cisco 15104 Optical Networking System Image Deferred

The regen-i6-mz image for the Cisco 15104 Optical Networking System has been deferred in Cisco IOS Release 12.2(4)T.

MPLS VPN with TE and MPLS InterAS Advisory on Cisco IOS Software

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) functionality is compromised for the following platforms in Cisco IOS Release 12.2(4)T:

- Cisco 3660 series and 3640 series
- Cisco 7200 series and 7500 series

- Cisco UBR7000 series
- Cisco RPM series

Refer to the advisory notice at the following location:

http://www-tac.cisco.com/Support_Library/field_alerts/fn15911.html.

Important Notes for Cisco IOS Release 12.2(2)T

The following information applies to Cisco IOS Release 12.2(2)T.

Addition of the squeeze Command for Cisco 2600 and Cisco 3600 Series Routers

The **squeeze** command, which is used to erase all files marked for deletion on a Flash file system, is now available on Cisco 2600 and Cisco 3600 series routers.

Changes to the output attenuation Command

In Cisco IOS Release 12.2(2), the range of the **output attenuation** command for voice ports has changed from *0–14* to *–6–14*.

Cisco 820 and SOHO 70 Router Images Deferred Because of Caveat CSCds69577

Six images in Cisco IOS Release 12.2(2)T and 12.2(2)T1 were deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCds69577. This caveat affects the following images:

- c820-k8osv6y6-mz
- c820-k8osy6-mz
- c820-nsv6y6-mz
- c820-v6y6-mz
- c820-y6-mz
- soho70-y1-mz

With caveat CSCds69577, connectivity to some web sites is lost when the router terminates PPP over Ethernet. The software solution for these deferred images is Cisco IOS Release 12.2(1)XD1, which is available on Cisco.com.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Cisco Catalyst 4000 Gateway Images Deferred Because of Caveats CSCdu59093 and CSCdu63022

Three images in Cisco IOS Release 12.2(2)T and 12.2(2)T1 were deferred because of severe defects. These defects have been assigned Cisco caveat ID CSCdu59093 and CSCdu63022. These caveats affect the following images:

- c4gwy-cboot-mz
- c4gwy-io3s-mz
- c4gwy-io3sx3-mz

With caveat CSCdu59093, a Catalyst 4000 Gateway may reload when a conference call is made. With caveat CSCdu63022, a Cisco Catalyst 4000 Gateway may not be able to be used as a conference bridge. The software solution for these deferred images is Cisco IOS Release 12.1(5)T9, which is available on Cisco.com.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Caveats for Cisco IOS Release 12.2 T

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

For information on caveats in Cisco IOS Release 12.2 T, refer to the *Caveats for Cisco IOS Release 12.2 T* document, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.2 T and is located on Cisco.com and the Documentation CD-ROM.

Note If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support**: **Software Center**: **Cisco IOS Software**: **BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Apêndice FZ

TECHNICAL SUPPORT

SNMP Object Navigator

Here is a list of MIBs that is supported by c1700-k9sv3y7-mz.12.2-15.T.

BRIDGE-MIB
CISCO-ATM-EXT-MIB
CISCO-MEMORY-POOL-MIB
CISCO-BULK-FILE-MIB
CISCO-PING-MIB
CISCO-CALL-HISTORY-MIB
CISCO-PROCESS-MIB
CISCO-CAR-MIB
OLD-CISCO-CPU-MIB
CISCO-QUEUE-MIB
CISCO-CDP-MIB
OLD-CISCO-INTERFACES-MIB
CISCO-RTTMON-MIB
SNMP-TARGET-MIB
CISCO-CONFIG-COPY-MIB
OLD-CISCO-IP-MIB
CISCO-SNAPSHOT-MIB
SNMP-USM-MIB
CISCO-CONFIG-MAN-MIB
OLD-CISCO-MEMORY-MIB
CISCO-SYSLOG-MIB
SNMP-VACM-MIB
CISCO-DIAL-CONTROL-MIB
OLD-CISCO-SYSTEM-MIB
XGCP-MIB
CISCO-TCP-MIB
SNMPv2-MIB
CISCO-FLASH-MIB
OLD-CISCO-TCP-MIB
CISCO-IPSEC-FLOW-MONITOR-MIB
CISCO-VOICE-ANALOG-IF-MIB
TCP-MIB
OLD-CISCO-TS-MIB
CISCO-IPSEC-MIB
CISCO-VOICE-DIAL-CONTROL-MIB
UDP-MIB
PIM-MIB
CISCO-IPSEC-POLICY-MAP-MIB
OLD-CISCO-FLASH-MIB
RFC1213-MIB
CISCO-PIM-MIB
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
RFC1253-MIB
CISCO-PRODUCTS-MIB
CISCO-CLASS-BASED-QOS-MIB
CISCO-IETF-NAT-MIB
CISCO-ICSUDSU-MIB
CISCO-ATM-PVCTRAP-EXTN-MIB
IPMROUTE-STD-MIB
CISCO-IETF-IP-FORWARD-MIB
CISCO-IETF-IP-MIB
CISCO-FRAME-RELAY-MIB
CISCO-FTP-CLIENT-MIB
CISCO-VOICE-IF-MIB
CISCO-H323-TC-MIB
CISCO-VPDN-MGMT-MIB

Related Tools

TAC Case Open
TAC Case Query
MIB Locator

CISCO-HSRP-EXT-MIB
DIAL-CONTROL-MIB
RFC1315-MIB
CISCO-HSRP-MIB
ENTITY-MIB
RFC1381-MIB
CISCO-IETF-ATM2-PVCTRAP-MIB
HC-RMON-MIB
CISCO-ISDNU-IF-MIB
RFC1382-MIB
CISCO-IMAGE-MIB
IF-MIB
CISCO-STACKMAKER-MIB
RFC1406-MIB
CISCO-IP-STAT-MIB
INT-SERV-GUARANTEED-MIB
CISCO-CALL-APPLICATION-MIB
RMON-MIB
CISCO-IPMROUTE-MIB
INT-SERV-MIB
CISCO-CAS-IF-MIB
RMON2-MIB
CISCO-ISDN-MIB
ISDN-MIB
CISCO-CIRCUIT-INTERFACE-MIB
RS-232-MIB
OLD-CISCO-CHASSIS-MIB
CISCO-NTP-MIB
RSVP-MIB
CISCO-VOICE-COMMON-DIAL-CONTROL-MIB
SMON-MIB
CISCO-VPDN-MGMT-EXT-MIB
SNMP-FRAMEWORK-MIB
ETHERLIKE-MIB
IGMP-STD-MIB
MSDP-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB
SNMP-NOTIFICATION-MIB
IP-FORWARD-MIB
CISCO-ENTITY-ASSET-MIB
CISCO-SIP-UA-MIB
CISCO-BGP4-MIB
CISCO-PPPOE-MIB
ATM-MIB
BGP4-MIB

BUSINESS INDUSTRIES & SOLUTIONS | NETWORKING SOLUTIONS & PROVISIONED SERVICES | PRODUCTS & SERVICES | TECHNOLOGIES | ORDERING | TECHNICAL SUPPORT | LEARNING & EVENTS | PARTNERS & RESELLERS | ABOUT CISCO
Home | Logged In | Profile | Contacts & Feedback | Site Help

individual host that is joined to a particular group or channel. The main benefits are that this feature provides minimal leave latencies, faster channel changing, and improved diagnostics capabilities for IGMP.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_xtrk.htm.

IKE—Initiate Aggressive Mode

The IKE—Initiate Aggressive Mode feature allows you to specify RADIUS Tunnel attributes (Tunnel-Client-Endpoint [66] and Tunnel-Password [69]) for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes. This feature is best implemented in a crypto hub-and-spoke scenario, in which the spokes initiate IKE aggressive mode negotiation with the hub by using the preshared keys that are specified as tunnel attributes and stored on the AAA server. This scenario is scalable because the preshared keys are kept at a central repository (the AAA server) and more than one hub router and one application can use the information.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ikeag.htm.

Integrated IS-IS Point-to-Point Adjacency Over Broadcast Media

When a network consists of only two networking devices that are connected to broadcast media and using the integrated IS-IS protocol, it is better for the system not to have to handle the link as a broadcast link but rather as a point-to-point link. The Integrated IS-IS Point-to-Point Adjacency Over Broadcast Media feature introduces a new command to make IS-IS behave as a point-to-point link between the networking devices.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftissp2p.htm.

Integrated IS-IS Support for IPv6

IPv6 supports Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs). Routing Information Protocol (RIP) and Integrated Intermediate System-to-Intermediate System (IS-IS) protocols are the supported IGPs for IPv6. Multiprotocol Border Gateway Protocol (BGP) is the supported EGP for IPv6.

IS-IS in IPv6 functions the same as and offers many of the same benefits as IS-IS in IPv4. IPv6 enhancements to IS-IS allow IS-IS to advertise IPv6 prefixes in addition to IPv4 and Open System Interconnection (OSI) routes. Extensions to the IS-IS CLI allow configuration of IPv6-specific parameters. IS-IS in IPv6 extends the address families supported by IS-IS to include IPv6, in addition to OSI and IPv4.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/ftipv6s.htm.

Interactive Voice Response Version 2.0 on VoIP Gateways

Interactive Voice Response (IVR) consists of simple voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination. IVR applications can be assigned to specific ports or invoked on the basis of dialed number identification service (DNIS). An IP Public Switched Telephone Network (PSTN) gateway can have several IVR applications to accommodate many different gateway services, and you can customize the IVR applications to present different interfaces to the various callers.

IVR systems provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words, or more commonly, dual tone multifrequency (DTMF) signaling. IVR uses Tool Command Language (TCL) scripts to gather information and to process accounting and billing.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ivr72.htm.

IP-FORWARDING-TABLE-MIB

This release introduces support for the new IP-FORWARD-MIB (IP Forwarding Table MIB). The current version of the IP Forwarding Table MIB is defined in RFC 2096. (RFC 2096 replaces RFC 1354.) The Cisco implementation of this MIB does not support the ipCiderRouteNextHopAS object. Additionally, all entries for the ipCidrRouteTos object (the IP Type-of-Service field) remain set to zero, which indicates a default TOS policy.

For details, refer to the IP-FORWARD-MIB.my file, available through the Cisco MIB FTP site at the following URL:

ftp://ftp.cisco.com/pub/mibs/v2/.

IP Multicast MIB Enhancements

The IP Multicast MIB Enhancements feature enhances the IP multicast routing protocol in Cisco IOS software by adding MIB variables to query the number of (S, G) and (*, G) entries. It also adds support for high-speed interface counters.

IPSec VPN High Availability Enhancements

The IPSec VPN High Availability feature consists of two new features—Reverse Route Injection and Hot Standby Router Protocol and IPSec—that work together to provide users with a simplified network design for VPNs and reduced configuration complexity on remote peers with respect to defining gateway lists.

Reverse Route Injection

Reverse Route Injection (RRI) is a feature designed to simplify network design for Virtual Private Network (VPNs) in which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

In the dynamic case, as remote peers establish IPSec security associations (SAs) with an RRI-enabled router, a static route is created for each subnet or host protected by that remote peer. For static crypto maps, a static route is created for each destination of an extended access-list rule.

HP Factory Express	*Factory Installation, Racking, and Customization Services*	
	Factory Express Server Configuration Level 1	293355-888
	NOTE: Free Installation of HP Options - Installation of HP Options memory, NICs, hard drives, controllers, processors, I/O cords, pre-install standard OEM OS image, and tape drives. Installation fees will apply to all non-HP certified hardware and asset tags. NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Server Configuration Level 2	266326-888
	NOTE: Includes Level 1 Customer Intent of a ProLiant server and options configuration, OS installation, custom image download, IP addressing, network setting, and custom packaging. Customer unique requirements (quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, and RILOE). Customer access, validation and control through VPN (price/server). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 3 with 1 - 3 servers or storage enclosures	325736-888
	Factory Express Rack Integration Level 3 with 4 - 9 servers or storage enclosures	232539-888
	Factory Express Rack Integration Level 3 with 10 or more servers or storage enclosures	325735-888
	NOTE: Includes Level 1 Customer Intent for standard mounted servers and storage units plus standard cable mgmt, RAID configuration, servers & storage, power distribution, networking gear and accessories (price/ra520ck). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 4 with 1 - 3 servers or storage enclosures	325734-888
	Factory Express Rack Integration Level 4 with 4 - 9 servers or storage enclosures	232540-888
	Factory Express Rack Integration Level 4 with 10 or more servers or storage enclosures	325733-888
	NOTE: Includes Level 2 Customer Intent plus customer defined cable management and naming convention, customer furnished image download, IP addressing, cluster configurations (SQL, External storage RAID). Quick restore creation, cd duplication, test reports, real-time reporting of server MAC address, password, RILOE). Customer access and validation through VPN (price/rack). NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
	Factory Express Rack Integration Level 5 with 1 - 3 servers or storage enclosures	325732-888
	Factory Express Rack Integration Level 5 with 4 - 9 servers or storage enclosures	232541-888
	Factory Express Rack Integration Level 5 with 10 or more servers or storage enclosures	325731-888
	NOTE: Includes Level 4 Customer Intent plus Custom SW layering and extended test, Customer access, validation and control through VPN, Clustered racks with networking gear and/or external storage array, Start-up installation services custom quote. (price/rack). NOTE: Factory Express Engineered Solution Level 6 is a custom solutions available through Factory Express. Please contact a your local reseller or Account Manager. NOTE: Available on ProLiant ML370 G3 Rack Models Only.	
Service and Support Offerings (HP Care Pack Services)	*Hardware Services On-site Service*	
	4-Hour On-site Service, 5-Day x 13-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL3EC-36
	4-Hour On-site Service, 5-Day x 13-Hour, 3 Years (U.S. Part Number)	331045-002
	4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-EL7EC-36
	4-Hour On-site Service, 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	162675-002
	6-Hour Call to Repair, On-site Service, 7-Day x 24-Hour Coverage, 3 Years (Canadian Part Number)	FP-ELCEC-36
	6-Hour Call to Repair, On-site Service 7-Day x 24-Hour Coverage, 3 Years (U.S. Part Number)	331046-002

Options

Installation & Start-up Services

Hardware Installation (Canadian Part Number)	FP-ELINS-EC
Hardware Installation (U.S. Part Number)	401791-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	240013-002
Installation & Start-Up of a ProLiant server and Microsoft O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (Canadian Part Number)	FM-MSTEC-01
Installation & Start-Up of a ProLiant server and Linux O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (U.S. Part Number)	331051-002
Installation & Start-Up of a ProLiant server and Linux O/S per the Customer Description and/or Data Sheet. To be delivered on a scheduled basis 8am-5pm, M-F, excl. HP holidays. (Canadian Part Number)	FM-LSTEC-01

Support Plus

Onsite HW support, 8am-9pm, M-F, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	239928-002
Onsite HW support, 8am-9pm, M-F, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-M01E1-36
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (U.S. Part Number)	331049-002
Onsite HW support, 8am-9pm, M-F, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 8am-9pm, M-F 2hr response time excl. HP holidays. (Canadian Part Number)	FM-L01E1-36

Support Plus 24

Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number)	239930-002
Onsite HW support 24x7, 4hr response and Microsoft O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canadian Part Number	FM-M02E1-36
Onsite HW support 24x7, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (U.S. Part Number	331050-002
Onsite HW support 24x7, 4hr response and Linux O/S SW Tech support offsite, onsite at HP's discretion, 24x7 2hr response time incl. HP holidays. (Canadian Part Number	FM-L02E1-36

CarePaq Priority Services for ProLiant Servers – Priority Silver

24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Manager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (2-5-2 Part Number for Canada)	FM-M04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (2-5-2 Part Number for Canada)	FM-M24E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (2-5-2 Part Number for Canada)	FM-N04E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (2-5-2 Part Number for Canada)	FM-N24E1-36
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System, Technical Account Manager, Technical Newsletter, SW activity review, proactive patch notification, 1 System Healthcheck per year (6-3 Part Number for U.S.)	239932-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Windows NT, Windows 2000, Professional, Server or Advanced Server Operating System (6-3 Part Number for U.S.)	239934-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Software Support, 1-hr response, Monday – Friday, 8AM – 5PM local time, 2-hr response after hours for Novell NetWare Operating System, Technical Account Manager, Technical Newsletter, SW activity review (6-3 Part Number for U.S.)	239972-002
24 x 7 HW, 4-hr response, Named HW engineer; 24 x 7 Silver Subsequent System Support for Novell NetWare Operating System (6-3 Part Number for U.S.)	239974-002

NOTE: For more information, customer/resellers can contact http://www.hp.com/services/carepack

Memory

HP ProLiant ML350 G3 Array Models

The ML350 G3 supports both interleaved and non-interleaved memory configurations. Array models ship standard with one 512MB DIMM, non-interleaved. Far best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory and installing in pairs is not required. Add any combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory

512MB (expandable to 8GB) of 2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models, with Advanced ECC capabilities (1x 512MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect and correct single bit memory errors while Advanced ECC extends this coverage to include protection against multiple simultaneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within a single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standard Memory Plus Optional Memory

Up to 6.7 GB of total memory can be implemented with the installation of three optional PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory

Up to 8.2 GB of total memory can be implemented with the removal of the standard 512-MB DIMM and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

NOTE: Charts do not represent all possible memory configurations.

		Slot 1	Slot 2	Slot 3	Slot 4
Standard	512 MB	512 MB	Empty	Empty	Empty
Optional	6656 MB	512 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB
2x1 Interleaved Memory (Recommended)		Pair 1		Pair 2	
	Total Memory	Slot 1	Slot 2	Slot 3	Slot 4
Recommended Configurations for Array Models	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

Following are memory options available from HP:

● 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
● 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21
● 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21
NOTE: To invoke interleaving in your array model, order this kit for a total of 1-GB of interleaved memory.	
● 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
● 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21

Memory

HP ProLiant ML350 G3 Non-Array Models
The ML350 G3 supports both interleoved and non-interleaved memory configurations. Base models ship standard with one 256MB DIMM, non-interleaved. For best performance automatically invoke interleaving by populating memory in identical pairs. Interleaving memory ond installing in pairs is not required. Add ony combination of memory DIMMs to operate in non-interleaved mode.

Standard Memory
256MB (expandable to 8GB) of 2-way interleaving capable PC2100 DDR SDRAM running at 200MHz on 400MHz models or 266MHz on 533MHz models with Advanced ECC capabilities (1x 256MB)

NOTE: Advanced ECC Memory - ECC protection provides the ability to detect and correct single bit memory errors while Advanced ECC extends this coverage to include protection against multiple simultoneous errors on a DIMM. Advanced ECC detects and corrects 4bit memory errors that occur within a single DRAM chip on a DIMM. Advanced ECC algorithms work in combination with industry standard ECC DIMMS.

Standard Memory Plus Optional Memory
Up to 6.4 GB optional memory is available with the installation of PC2100-MHz Registered ECC DDR SDRAM DIMMs.

Standard Memory Replaced with Optional Memory
Up to 8.2 GB of memory is available with the removal of the standard 256-MB of memory and the optional installation of PC2100-MHz Registered ECC DDR SDRAM DIMM installed.

NOTE: Charts do not represent all possible memory configurations

Memory					
		Slot 1	Slot 2	Slot 3	Slot 4
Standard	256 MB	256 MB	Empty	Empty	Empty
Optional	6400 MB	256 MB	2048 MB	2048 MB	2048 MB
Maximum	8192 MB	2048 MB	2048 MB	2048 MB	2048 MB
Recommended Configurations for Base Models	Total Memory Desired	1	2	3	4
	512 MB	256 MB	256 MB	Empty	Empty
	1 GB	256 MB	256 MB	256 MB	256 MB
	1.5 GB	256 MB	256 MB	512 MB	512 MB
Recommended Configurations for Array models	Total Memory Desired	1	2	3	4
	1 GB	512 MB	512 MB	Empty	Empty
	1.5 GB	512 MB	512 MB	256 MB	256 MB
	2 GB	512 MB	512 MB	512 MB	512 MB

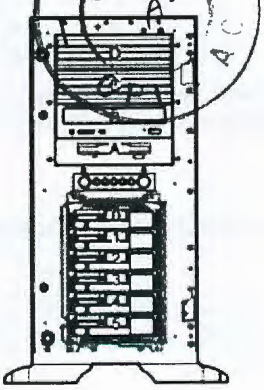
Following are memory options available from HP:

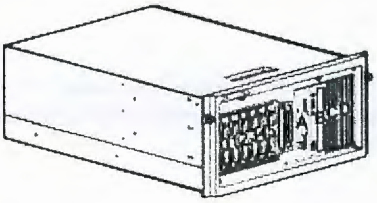
● 128MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 128 MB)	287494-B21
● 256MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 256 MB)	287495-B21

NOTE: To invoke interleaving in your base model, order this kit for a total of 512MB of interleaved memory.

● 512MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 512 MB)	287496-B21
● 1024MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 1024 MB)	287497-B21
● 2048MB of Advanced ECC PC2100 DDR SDRAM DIMM Memory Kit (1 x 2048 MB)	301044-B21

Storage





0 - 5	6 x 1 in SCSI Hard Drive Bays
A	3.5 in Diskette Drive
B	48x CD-ROM
C, D	Available half height bay

Drive Support

	Quantity Supported	Position Supported	Controller
Removable Media			
1.44-MB Diskette Drive	Up to 1	A	Integrated
IDE (ATAPI) CD-ROM Drive	Up to 2	B, C, D	Integrated IDE (ATAPI)
DVD-ROM Drive Option Kit	Up to 2	B, C, D	Integrated IDE
ML3xx Two Bay Hot Plug SCSI Drive Cage	Up to 1	C, D	Integrated SCSI

Storage

Hard Drives

Ultra320 Hot Pluggable Drives

	Quantity Supported	Position Supported	Controller
1-inch 146.8-GB 10,000 rpm 72.8-GB 10,000 rpm 36.4-GB 10,000 rpm 72.8-GB 15,000 rpm 36.4-GB 15,000 rpm 18.2-GB 15,000 rpm	Up to 6	0-5	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

NOTE: All U320 Universal Hard Drives are backward compatible to U2 or U3 speeds. U320 drives require an optional U320 Smart Array Controller or U320 SCSI HBA to support U320 transfer rates.

Wide Ultra320 SCSI – Non-Hot Plug

	Quantity Supported	Position Supported	Controller
1-inch 36-GB 10,000 rpm	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Compaq RAID LC2 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

External Storage

	Quantity Supported	Position Supported	Controller
StorageWorks Enclosure 4300 Family (supports Ultra3/Ultra320 1" drives)	Up to 24	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
3U Rackmount Kit 5U Rackmount Kit	Up to 3	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
MSA 1000	Please see the MSA 1000 QuickSpecs below to determine configuration requirements	External	Please see the MSA 1000 QuickSpecs (URL below) for the latest list of supported HBAs

MSA 1000: http://www5.compaq.com/products/quickspecs/11033_na/11033_na.HTML

Storage

Maximum Storage Capacity – (StorageWorks Enclosure)

Internal	1.174 TB (6 x 146.8-GB 1" Ultra320 hot plug hard drives with standard internal drive cage + 2 x 72.8-GB 1"Ultra320 Hot plug hard drive using the optional ML3xx Two Bay Hot Plug SCSI Drive Cage)
External	49.324 TB (14 x 146.8 GB) x 24
Total	50.498 TB

Tape Drives

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Drives listed below, please see the following: http://www5.compaq.com/products/quickspecs/North_America/10233.html

NOTE: For an up-to-date listing of the latest O/S Support details for each of the Tape Storage Systems listed below, please see the following: http://www5.compaq.com/products/quickspecs/North_America/10809.html

	Quantity Supported	Position Supported	Controller
Internal AIT 100-GB, Hot Plug Internal AIT 50-GB, Hot Plug Internal AIT 35-GB, LVD Hot Plug Internal 20/40-GB DAT Drive, Hot Plug Internal DAT 72, Hot Plug *Installation of AIT/DAT hot plug drives in D+C requires the optional Two Bay Hot Plug SCSI Drive Cage (PN 244059-B21)	Up to 3	0+ 1, 2+ 3, D+ C*	Smart Array 532 Controller Smart Array 5302/128 Controller Smart Array 5304/256 Controller Smart Array 5312 Controller Smart Array 641 Controller (NOTE: The Smart Array 641 ships standard with 2.8 GHz Array models.) Smart Array 642 Controller 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter *NOTE: The Smart Array 532 Controller does not support the AIT 100-GB Hot Plug Tape Drive.
20/40-GB DAT DDS-4 Tape Drive Internal 12/24-GB DAT Drive Internal DAT 72	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 35GB, Autoloader	Up to 4	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT Enhanced	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
Internal 40/80-GB DLT VS	Up to 2	C, D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB Internal AIT 50-GB Internal AIT 35-GB, LVD Internal	Up to 2	C, D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 230, Internal LTO Ultrium 460, Internal	Up to 1	C + D	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SDLT 110/220-GB, Internal SDLT 160/320-GB, Internal	Up to 1	C + D	Integrated Dual Channel Wide Ultra3 SCSI Adapter 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External DAT 72	2	External	64-Bit/133-MHz Dual Channel Ultra320 SCSI Adapter
AIT 100-GB External AIT 50-GB External AIT 35-GB, LVD External	2	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
External 40/80-GB DLT Enhanced External 40/80-GB DLT VS External 20/40-GB DLT	Up to 3	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
LTO Ultrium 215, External LTO Ultrium 230, External LTO Ultrium 460, External	Up to 2	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter

Storage

SDLT 110/220-GB, External SDLT 160/320-GB, External	Up to 2	External	Integrated Dual Channel Wide Ultra3 SCSI Adapter (requires Internal-to-External SCSI cable option) 64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
20/40-GB DAT 8 Cassette Autoloader External	Up to 1	External	64-Bit/133Mhz Dual Channel Ultra320 SCSI Adapter
SSL2020 AIT Library	2 drives per SCSI channel	External	SAN Access Module for Smart Array 5302 Controller
MSL5026DLX (40/80GB DLT-based) MSL5026SL (SDLT-based) Library MSL5052SL (SDLT-based) Library MSL5030L (LTO-based) Library MSL5060S (LTO-based) Library	2 drives per SCSI channel	External	64-Bit/66-MHz Dual Channel Wide Ultra3 SCSI Adapter, Alternate OS

Power Specifications

Part Number	264166-001
Spare Kit	292237-001
Operational Input Voltage Range (V rms)	90 to 264
Frequency Range (Nominal) (Hz)	47 to 63 (50/60)

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Max Rated Output Wattage Rating	500	500	500	500	500	500
Nominal Input Current (A rms)	7.8	6.7	3.7	3.4	3.2	3.0
Max Rated Input Wattage Rating (Watts)	769	758	746	735	725	714
Max. Rated VA (Volt-Amp)	785	773	761	750	739	729
Efficiency (%)	65	66	67	68	68	70
Power Factor	0.98	0.98	0.98	0.98	0.98	0.98
Leakage Current (mA)	0.31	0.36	0.65	0.69	0.72	0.75
Maximum Inrush Current (A peak)	21	24	43	46	48	50
Maximum Inrush Current duration (miliseconds)	20	20	20	20	20	20

System Specifications

ML350 Generation 3 (G3) Fully Configured

Up to 2 Processors, 4 Memory Slots, 8 Hard Drives, 5 PCI Slots, and 2 Hot Plug Power Supplies

Nominal Input Voltage (Vrms)	100	115	208	220	230	240
Fully Loaded System Input Wattage (W)	557	549	541	534	526	519
Fully Loaded System Input Current (A rms)	5.7	4.9	2.7	2.5	2.3	2.2
Fully Loaded System Thermal (BTU-Hr)	1900	1872	1846	1820	1794	1770
Fully Loaded System VA (Volt-Amp)	569	560	552	545	537	530
System Leakage with all power supplies loaded (mA)	0.63	0.72	1.30	1.38	1.44	1.50
System Inrush Current with all power supplies loaded (A)	42	48	86	92	96	100
Power cord requirements	Nema 5-15P to IEC320-C13			Option no./Spare no: See Power Cord chart		
	IEC320-C13 to IEC320-C14			Option no./Spare no: 142257-001/142258-B21		

NOTES:
ActiveAnswers Power Calculation
Power colculotor is LIVE on ActiveAnswers Web site. This is on external link.
Follow this link: http://h30099.www3.hp.com/configurator/powercalcs.asp
NOTE: This Web site is available in English only.

To drill down to calculators:
- Click on: "ProLiant Servers"
- Click on the Server of interest. Example: ML350 G3
- Click on: "Power Calculator" link. (You may need to scroll down to see it)

TechSpecs

System Unit – Tower	Dimensions (HxWxD) (with feet/bezel)	18.5 x 10.25 x 26 in (46.99 x 26.04 x 66.04 cm)	
	Dimensions (HxWxD) (without feet/bezel)	17.5 x 8.5 x 24 in (44.50 x 21.59 x 60.96 cm)	
	Weight(approximate)	60 lb (27.24 kg) (without hard drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors (Support for either two internal, two external, or a mix of internal/external is available. This is achieved using an internal to external SCSI cable option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	500W
	Temperature Range	Operating	50° to 95° F (10° to 35° C) (No direct sustaining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

TechSpecs

System Unit – Rack	Dimensions (HxWxD)	8.61 x19 x 24 in (21.87 x48.26 x 60.96 cm)	
	Weight(approximate)	60 lb (27.24 kg) (without hard drives)	
	Input Requirements (per power supply)	Range Line Voltage	100 to 120 VAC/200 to 240 VAC
		Rated Input Frequency	50 Hz to 60 Hz
		Input Power	538W @ 110 VAC
		Rated Input Current	7.4A/3.7A
	Line Frequency	50 to 60 Hz	
	BTU Rating	1, 839 BTU/hr	
	SCSI Connectors	Two internal HD68 connectors (Support for either two internal, two external, or a mix of internal/external is available. This is achieved using an internal to external SCSI cable option kit (PN 159547-B22) and either of the two SCSI knockouts.)	
	Power Supply Output Power (per power supply)	Rated Steady-State Power	500W
	Temperature Range	Operating	50° to 95° F (10° to 35° C) (No direct sustaining sunlight)
		Storage (up to one year)	-40° to 158° F (-40° to 70° C)
	Maximum Wet Bulb Temperature	82.4° F (28° C)	
	Relative Humidity (non-condensing)	Operating	10% to 90%
		Non-operating	5% to 90%
	Acoustic Noise	Idle (Fixed Disk Drives Spinning)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.3
		Operating (Random Seeks to Fixed Disks)	
		L WAd (BELS)	6.0
		L pAm (dBA)	46.5

1.44-MB Diskette Drive	LED Indicators (front panel)	Green	
	Read/Write Capacity per Diskette (high/low density)	1.44 MB/720 KB	
	Drive Supported	One	
	Drive Height	One-third	
	Drive Rotation	300 rpm	
	Transfer Rate (high/low)	500 K/250 K bits/s	
	Bytes/Sector	512	
	Sectors/Track (high/low)	18/9	
	Tracks/Side (high/low)	80/80	
	Access Times	Track-to-Track (high/low)	3/6 ms
		Average (high/low)	169/94 ms
		Settling Time	15 ms
		Latency Average	100 ms
	Cylinders (high/low)	80/80	
	Read/Write Heads	Two	

48X Max IDE (ATAPI) CD-ROM Drive	Disk	Applicable Disk	CD-ROM, CD-XA, CD-DA (Mode 1, Mode 2, Form 1 and 2) Photo CD (Single and Multi-session) Mixed Mode (Audio and Data combined) CD-R
		Capacity	540 MB (Mode 1, 12 cm) 650 MB (Mode 2, 12 cm)
	Block Size	Mode 1	2,048 bytes
		Mode 2	2,340 bytes, 2,336 bytes
		CD-DA	2,352 bytes
		CD-XA	2,328 bytes
	Interface	IDE (ATAPI)	
	Access Times (typical)	Random	<100 ms
		Full-Stroke	<150 ms
	Data Transfer Rate	Sustained	3000 to 7200 KB/s (20X to 48X)
		Burst	150 KBps to 7,200 KBps
		Bus Rate	16.7 MBps
	Cache Buffer	128 KB	
	Start-up Time (typical)	< 7seconds	
	Stop Time	< 4seconds	
	Laser Parameters	Type	Semiconductor Laser GaA1As
		Wave Length	780 ± 25 nm
	Operating Conditions	Temperature	41° to 113° F (5° to 45° C)
		Humidity	10% to 80%
	Dimensions	(HxWxD, maximum)	1.7 x 5.85 x 8.11 in (4.29 x 14.86 x 20.60 cm)
		Weight	2.09 lb (0.95 kg)

NC7760 PCI Gigabit Server Adapter (embedded)	Network Interface	10Base-T/100Base-TX/1000Base-TX	
	Compatibility	IEEE 802.3 10Base-T IEEE 802.3ab 1000Base-T IEEE 80.3u 100Base-TX	
	Data Transfer Method	32-bit bus-master PCI	
	Network Transfer Rate	10Base-T(Half-Duplex)	10 Mb/s
		10Base-T(Full-Duplex)	20 Mb/s
		100Base-TX(Half-Duplex)	100 Mb/s
		100Base-TX(Full-Duplex)	200 Mb/s
		1000Base-TX	1000Mb/s
	Connector	RJ-45	
	Cable Support	10Base-T	Categories 3, 4 or 5 UTP; up to 328 ft (100 m)
		10/100/1000Base-TX	Category 5 UTP; up to 328 ft (100 m)

TechSpecs

Integrated Dual Channel Wide Ultra3 SCSI Adapter	Drives Supported	Up to 28 SCSI devices (14 per channel)
	Data Transfer Method	64-bit PCI bus-master
	SCSI Channel Transfer Rate	80 MB/s per channel
	Maximum Transfer Rate per PCI Bus (peak)	133 MB/s per channel
	SCSI Protocols	Wide Ultra2 SCSI Wide-Ultra SCSI-3 Fast SCSI-2
	Electrical Protocol	Low Voltage Differential (LVD)
	SCSI Termination	Active Termination
	External SCSI Connectors	Two 80-Pin VHDCI connectors
	Internal SCSI Connectors	Two 68-Pin Wide-Ultra SCSI-3 connectors

Smart Array 641 Controller (NOTE: The Smart Array 641 Controller ships standard with the 2.8 GHz Array Models only)	Protocol	Ultra320 SCSI
	SCSI Electrical Interface	Low Voltage Differential (LVD)
	Drives Supported	Up to 6 Ultra 320, Ultra3 and Ultra2 SCSI hard drives
	SCSI Port Connectors SA-641	one internal SCSI port
	Data Transfer Method	64-Bit PCI bus-master
	PCI Bus Speed	64-bit, 133-MHz PCI-X (1 GB/s maximum bandwidth)
	PCI	3.3 volt PCI slot compatibility only
	Simultaneous Drive Transfer Channels	Two
	Channel Transfer Rate	320-MB/s total; 320-MB/s per channel
	Software upgradeable Firmware	Yes
	Cache Memory	64-MB DRAM used for code, transfer buffers, and non-battery backed read cache
	Logical Drives Supported	32
	Maximum Capacity	880.8 GB (6 X 146.8 GB)
	Memory Addressing	64-bit, supporting servers memory greater than 4 GB
	RAID Support	RAID 5 (Distributed Data Guarding) RAID 1+ 0 (Striping & Mirroring) RAID 1 (Mirroring) RAID 0 (Striping)
	Upgradeable Firmware	2-MB Flashable ROM
	Disk Drive and Enclosure Protocol Support	Ultra 320, Ultra2 and Ultra3
	Warranty	Maximum: The remaining warranty of the HP server product in which it is installed (to a maximum three-year limited warranty) Minimum: One-year, on-site limited warranty Pre-Failure Warranty: Drives attached to the Smart Array Controller and monitored under Insight Manager are supported by a Pre-Failure (replacement) Warranty. For complete details, consult the HP Support Center or refer to your HP Server Documentation.

TechSpecs

Video Controller	Controller Chip	ATI RAGE XL
	Video DRAM	8 MB Video SDRAM
	Data Transfer Method	32-bit PCI
	Support Resolution	Supported Color Depths:
	640 x 480	16.7M, 64K, 256, 16
	800 x 600	16.7M, 64K, 256, 16
	1024 x 768	16.7M, 64K, 256, 16
	1152 x 864	16.7M, 64K, 256, 16
	1280 x 1024	16.7M, 64K, 256, 16
	1600 x 1200	64K, 256, 16
	Connector	VGA

The information contained herein is subject to change without notice.

Microsoft and Windows NT are US registered trademarks of Microsoft Corporation. Intel is a US registered trademark of Intel Corporation.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Apêndice FP

CISCO SYSTEMS

Data Sheet

Cisco PIX **535** Security Appliance

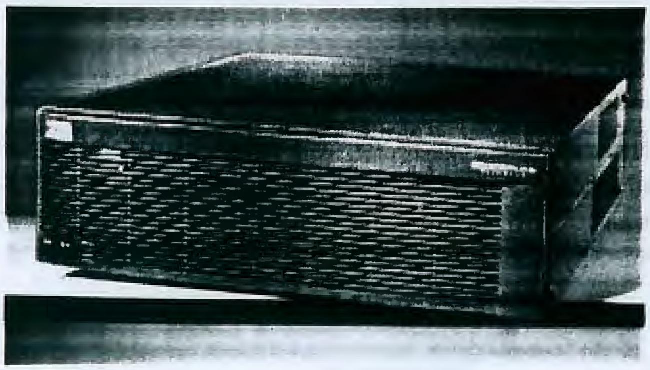
The Cisco PIX® 535 Security Appliance delivers enterprise-class security for enterprise and service provider networks in a high performance, purpose-built appliance. Its highly modular three-rack unit (3RU) design supports up to ten 10/100 Fast Ethernet interfaces or nine Gigabit Ethernet interfaces as well as redundant power supplies, making it an ideal choice for businesses requiring the highest levels of performance, port density, reliability, and investment protection. Part of the world-leading Cisco PIX Security Appliance Series, the Cisco PIX 535 Security Appliance provides a wide range of rich integrated security services, hardware VPN acceleration capabilities, and powerful remote management capabilities in a highly scalable, high-performance solution.

Enterprise-Class Security for Large Enterprise and Service Provider Networks

The Cisco PIX 535 Security Appliance delivers a multilayered defense for enterprise and service provider networks through rich, integrated security services including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN) in-line intrusion protection, and rich multimedia and voice security in a single device. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access.

Enterprise networks benefit from an additional layer of security via intelligent, "application-aware" security services that examine packet streams at Layers 4–7, using inspection engines specialized for many of today's popular applications. Administrators can also easily create custom security policies for firewall traffic by using the flexible access control methods and the more than 100 predefined applications, services, and protocols that Cisco PIX Security Appliances provide.

Figure 1
Cisco PIX 535 Security Appliance



Market-Leading Voice-over-IP Security Services Protect Next-Generation Converged Networks

Cisco PIX Security Appliances provide market-leading protection for a wide range of voice-over-IP (VoIP) and multimedia standards, allowing businesses to securely take advantage of the many benefits that converged data, voice, and video networks deliver. By combining VPN with the rich stateful inspection firewall services that Cisco PIX Security Appliances provide for these converged networking standards, businesses can securely extend voice and multimedia services to home office and remote office environments for additional cost savings, improved productivity, and competitive advantage.

Flexible VPN Services Extend Networks Economically to Remote Networks and Mobile Users

Businesses can securely extend their networks across low-cost Internet connections to mobile users, business partners, and remote offices worldwide using the full-featured VPN capabilities provided by the Cisco PIX 535 Security Appliance. Solutions range from standards-based site-to-site VPN leveraging the Internet Key Exchange (IKE) and IP security (IPsec) VPN standards, to the innovative Cisco Easy VPN capabilities found in Cisco PIX Security Appliances and other Cisco security solutions—such as Cisco IOS® routers and Cisco VPN 3000 Series Concentrators. Easy VPN delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture that eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Cisco PIX Security Appliances encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced Encryption Standard (AES) encryption. Certain Cisco PIX 535 Security Appliance models have integrated hardware VPN acceleration capabilities, delivering highly scalable, high performance VPN services.

Integrated Intrusion Protection Guards Against Popular Internet Threats

The integrated in-line intrusion-protection capabilities of the Cisco PIX 535 Security Appliance can protect enterprise networks from many popular forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Security Appliances keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time.

Award-Winning Resiliency Provides Maximum Business Uptime

Select models of Cisco PIX 535 Security Appliances provide stateful failover capabilities that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby, high-availability architecture, Cisco PIX Security Appliances that are configured as a failover pair continuously synchronize their connection state and device configuration data. Synchronization can take place over a high-speed LAN connection, providing another layer of protection through the ability to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned between appliances, with complete transparency to users.

Robust Remote-Management Solutions Lower Total Cost of Ownership

The Cisco PIX 535 Security Appliance is a reliable, easy-to-maintain platform that provides a wide variety of methods for configuring, monitoring, and troubleshooting. Management solutions range from centralized, policy-based management tools to integrated, Web-based management to support for remote monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog.

Administrators can easily manage large numbers of remote Cisco PIX Security Appliances using CiscoWorks VPN/ Security Management Solution (VMS). This suite consists of numerous modules including Management Center for Firewalls, Auto Update Server Software and Security Monitor. This powerful combination provides a highly scalable, next-generation, three-tier management solution that includes the following features:

- Comprehensive configuration and software image management
- Device hierarchy with "Smart Rules"-based configuration inheritance
- Customizable administrative roles and access privileges
- Comprehensive enterprise change management and auditing
- "Touchless" software image management for remote Cisco PIX Security Appliances
- Support for dynamically addressed appliances

Additional integrated event management and inventory solutions are also available as part of the CiscoWorks VMS network management suite.

The integrated Cisco PIX Device Manager provides an intuitive, Web-based management interface for remotely configuring, monitoring, and troubleshooting a Cisco PIX 535 Security Appliance—without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. A setup wizard is provided for easy installation into any network environment.

Alternatively, through methods including Telnet and Secure Shell (SSH), or out of band through a console port, administrators can remotely configure, monitor, and troubleshoot Cisco PIX Security Appliances using a command-line interface (CLI).

Table 1 Key Product Features and Benefits

Key Features	Benefit
Enterprise-Class Security	
True security appliance	• Uses a proprietary, hardened operating system that eliminates security risks associated with general purpose operating systems • Cisco quality and no moving parts provide a highly reliable security platform
Stateful inspection firewall	• Provides perimeter network security to prevent unauthorized network access • Uses state-of-the-art Cisco ASA for robust stateful inspection firewall services • Provides flexible access-control capabilities for over 100 predefined applications, services and protocols, with the ability to define custom applications and services • Includes numerous application-aware inspection engines that secure advanced networking protocols such as H.323 Version 4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), Internet Locator Service (ILS), and more • Includes content filtering for Java and ActiveX applets
Easy VPN Server	• Provides remote access VPN concentrator services for a wide variety of Cisco software or hardware-based VPN clients • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions upon connection, ensuring the latest corporate security policies are enforced • Extends VPN reach into environments using Network Address Translation (NAT) or Port Address Translation (PAT), via support of Internet Engineering Task Force (IETF) UDP-based draft standard for NAT traversal

Table 1 Key Product Features and Benefits

Key Features	Benefit
Site-to-site VPN	• Supports IKE and IPsec VPN standards • Ensures data privacy/integrity and strong authentication to remote networks and remote users over the Internet • Supports 56-bit DES, 168-bit 3DES and up to 256-bit AES data encryption to ensure data privacy
Intrusion protection	• Provides protection from over 55 different types of popular network-based attacks ranging from malformed packet attacks to DoS attacks • Integrates with Cisco Network Intrusion Detection System (IDS) sensors for the ability to dynamically block/shun hostile network nodes via the firewall
AAA support	• Integrates with popular authentication, authorization, and accounting services via TACACS+ and RADIUS support • Provides tight integration with Cisco Secure Access Control Server (ACS)
X.509 certificate and CRL support	• Supports SCEP-based enrollment with leading X.509 solutions from Baltimore, Entrust, Microsoft, and VeriSign
Integration with leading third-party solutions	• Supports the broad range of Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions that provide URL filtering, content filtering, virus protection, scalable remote management, and more
Robust Network Services/Integration	
Virtual LAN (VLAN)-based virtual interfaces	• Provides increased flexibility when defining security policies and eases overall integration into switched network environments by supporting the creation of logical interfaces based on IEEE 802.1q VLAN tags, and the creation of security policies based on these virtual interfaces • Supports multiple virtual interfaces on a single physical interface through VLAN trunking • Supports multiple VLAN trunks per Cisco PIX Security Appliances • Supports up to 24 VLANs on Cisco PIX 535 Security Appliances
Open Shortest Path First (OSPF) dynamic routing	• Provides comprehensive OSPF dynamic routing services using technology based on world-renowned Cisco IOS Software • Offers improved network reliability through fast route convergence and secure, efficient route distribution • Delivers a secure routing solution in environments using NAT through tight integration with Cisco PIX Security Appliance NAT services • Supports MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks • Provides route redistribution between OSPF processes, including OSPF, static, and connected routes • Supports load balancing across equal-cost multipath routes
DHCP server	• Provides DHCP Server services one or more interfaces for devices to obtain IP addresses dynamically • Includes extensions for support of Cisco IP Phones and Cisco SoftPhone IP telephony solutions
DHCP relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, enabling centralized distribution, tracking, and maintenance of IP addresses
NAT/PAT support	• Provides rich dynamic/static NAT and PAT capabilities

Table 1 Key Product Features and Benefits

Key Features	Benefit
Rich Management Capabilities	
CiscoWorks VPN/ Security Management Solution (CiscoWorks VMS)	• Comprehensive management suite for large scale deployments • Integrates policy management, software maintenance, and security monitoring
PIX Device Manager (PDM)	• Intuitive, Web-based GUI enables simple, secure remote management of Cisco PIX Security Appliances • Provides wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events
Auto Update	• Provides "touchless" secure remote management of Cisco PIX Security Appliance configuration and software images via a unique push/pull management model • Next-generation secure XML/HTTPS management interface can be leveraged by Cisco and third-party management applications for remote Cisco PIX Security Appliance configuration management, inventory, software image management/deployment and monitoring • Integrates seamlessly with Management Center for Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 Cisco PIX Security Appliances (per management server)
Cisco PIX CLI	• Allows customers to use existing PIX CLI knowledge for easy installation and management without additional training • Accessible through variety of methods including console port, Telnet and SSH
Command-level authorization	• Enables businesses to create up to 16 customizable administrative roles/profiles for accessing Cisco PIX Security Appliances (for example, monitoring only, read-only access to configuration, VPN administrator, firewall/NAT administrator, and so on) • Leverages either the internal administrator database or outside sources via TACACS+, such as Cisco Secure ACS
SNMP and syslog support	• Provide remote monitoring and logging capabilities, with integration into Cisco and third-party management applications
Highly Flexible Expansion Capabilities	
Fast Ethernet and Gigabit Ethernet expansion options	• Supports easy installation of additional network interfaces via four 66-Mhz/64-bit and 5 33-MHz/32-bit PCI expansion slots • Supports expansion cards including single-port Fast Ethernet card, 4-port Fast Ethernet card, and single-port Gigabit Ethernet card
Hardware VPN acceleration options	• Delivers high speed VPN services via support of VPN Accelerator Card (VAC) and VPN Accelerator Card+ (VAC+)

License Options

The Cisco PIX 535 Security Appliance is available in three primary models that provide different levels of interface density, failover capabilities, and VPN throughput.

Restricted Software License

The Cisco PIX 535 "Restricted" (PIX 535-R) model provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with gigabit firewall throughput, high interface density, maximum investment protection, and moderate VPN throughput requirements. It includes 512 MB of RAM and support for up to eight 10/100 Fast Ethernet or eight Gigabit Ethernet interfaces.

Unrestricted Software License

The PIX 535 "Unrestricted" (PIX 535-UR) model extends the capabilities of the family with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleratio It includes an integrated VAC or VAC+ hardware VPN accelerator, 1 GB of RAM, and support for up to ten 10/1 Fast Ethernet or nine Gigabit Ethernet interfaces. The Cisco PIX 535-UR also adds the ability to share state information with a hot-standby Cisco PIX Security Appliance for resilient network protection.

Failover Software License

The Cisco PIX 535 "Failover" (PIX 535-FO) model is designed for use in conjunction with a PIX 535-UR, providing a cost-effective, high-availability solution. It operates in hot-standby mode acting as a complete redundant system that maintains current session state information. With the same hardware configuration as the Cisco PIX 535-UR, it delivers the ultimate in high availability for a fraction of the price.

Performance Summary

Cleartext throughput: 1.7 Gbps

Concurrent connections: 500,000

168-bit 3DES IPsec VPN throughput: Up to 440 Mbps with VAC+ or 100 Mbps with VAC

128-bit AES IPsec VPN throughput: Up to 535 Mbps with VAC+

256-bit AES IPsec VPN throughput: Up to 440 Mbps with VAC+

Simultaneous VPN tunnels: 2000

Technical Specifications

Processor: 1-GHz Intel Pentium III Processor

Random access memory: 512 MB or 1 GB of SDRAM

Flash memory: 16 MB

Cache: 256 KB level 2 at 1-GHz

System buses: Two 64-bit, 66 MHz PCI, one 32-bit, 33-MHz PCI

Environmental Operating Ranges

Operating

Temperature: –25° to 131°F (-5° to 55°C)

Relative Humidity: 5% to 95%, noncondensing

Altitude: 0 to 9843 ft (3000 m)

Shock: 1.14 m/sec (45 in./sec) 1/2 sine input

Vibration: 0.41 Grms2 (3–500 Hz) random input

Acoustic Noise: 65 dBa maximum

Nonoperating

Temperature: –13° to 158°F (–25° to 70°C)

Relative Humidity: 5% to 95%, noncondensing

Altitude: 0 to 15,000 ft (4570 m)

Shock: 30 G

Vibration: 0.41 Grms2 (3–500 Hz) random input

Power

Input (per power supply)

Range Line Voltage: 100V to 240V AC or 48V DC

Nominal Line Voltage: 100V to 240V AC or 48V DC

Current: 4–2 Amps

Frequency: 50 to 60 Hz, single phase

Power: 220W (dual hot swap power supply capable)

Output

Steady State: 135W

Maximum Peak: 220W

Maximum Heat Dissipation: 750 BTU/hr, full power usage (220W)

Physical Specifications

Dimensions and Weight Specifications

Form factor: 3 RU, standard 19-in. rack mountable

Dimensions (H x W x D): 5.25 x 17.5 x 18.25 in. (13.33 x 44.45 x 46.36 cm)

Weight (one power supply): 32 lb (14.5 kg)

Expansion

Four 64-bit/66-MHz PCI slots

Five 32-bit/33-MHz PCI slots

Six 168-pin DIMM RAM slots, supporting up to 1 GB PC133 DRAM

Interfaces

Console Port: RS-232 (RJ-45) 9600 baud

Failover Port: RS-232 (DB-15) 115 Kbps (Cisco specified cable required)

Two integrated 10/100 Fast Ethernet ports, auto-negotiate (half/full duplex), RJ-45

Regulatory and Standards Compliance

Safety

UL 1950, CSA C22.2 No. 950, EN 60950, IEC 60950, AS/NZS3260, TS001, IEC60825, EN 60825, 21CFR1040

Electro Magnetic Compatibility (EMC)

FCC Part 15 (CFR 47) Class A, ICES 003 Class A with UTP, EN55022 Class A with UTP, CISPR 22 Class A with UTP, AS/NZ 3548 Class A with UTP, VCCI Class A with UTP, EN55024, EN50082-1 (1997), CE marking, EN55022 Class B with FTP, Cispr 22 Class B with FTP, AS/NZ 3548 Class B with FTP, VCCI Class B with FTP

Product Ordering Information

PIX-535	PIX 535 chassis only
PIX-535-R-BUN	PIX 535 restricted bundle (chassis, restricted software, 2 10/100 ports, 512 MB RAM)
PIX-535-UR-BUN	PIX 535 unrestricted bundle (chassis, unrestricted software, 2 10/100 ports, 1 GB RAM, VAC or VAC+)
PIX-535-FO-BUN	PIX 535 failover bundle (chassis, failover software, 2 10/100 ports, 1 GB RAM, VAC or VAC+)
PIX-535-HW=	PIX 535 rack mount kit, console cable, failover serial cable
PIX-FO=	PIX failover serial cable
PIX-4FE	4-port 10/100 Fast Ethernet PCI expansion card
PIX-1FE	Single-port 10/100 Fast Ethernet PCI expansion card
PIX-1GE-66	Single-port Gigabit Ethernet 64-bit/66-MHz PCI expansion card, Multimode (SX) SC connector
PIX-VPN-ACCEL	3DES IPsec hardware VAC
PIX-VAC-PLUS	3DES/AES IPsec hardware VAC+
PIX-VPN-3DES	168-bit 3DES and up to 256-bit AES encryption software license

PIX-VPN-3DES=	168-bit 3DES and up to 256-bit AES encryption software license
PIX-VPN-DES	56-bit DES encryption software license
PIX-VPN-DES=	56-bit DES encryption software license

Support Services

Support services are available from Cisco and Cisco partners. Cisco SMARTnet service augments customer support resources, and provides anywhere, anytime access to technical resources (both online and by telephone), the ability to download updated system software, and hardware advance replacement.

Support Ordering Information

CON-SNT-PIX535	SMARTnet 8x5xNBD service for PIX 535 chassis only
CON-SNT-PIX535R	SMARTnet 8x5xNBD service for PIX 535-R bundle
CON-SNT-PIX535UR	SMARTnet 8x5xNBD service for PIX 535-UR bundle
CON-SNT-PIX535FO	SMARTnet 8x5xNBD service for PIX 535-FO bundle
CON-SNTE-PIX535	SMARTnet 8x5x4 service for PIX 535 chassis only
CON-SNTE-PIX535R	SMARTnet 8x5x4 service for PIX 535-R bundle
CON-SNTE-PIX535UR	SMARTnet 8x5x4 service for PIX 535-UR bundle
CON-SNTE-PIX535FO	SMARTnet 8x5x4 service for PIX 535-FO bundle
CON-SNTP-PIX535	SMARTnet 24x7x4 service for PIX 535 chassis only
CON-SNTP-PIX535R	SMARTnet 24x7x4 service for PIX 535-R bundle
CON-SNTP-PIX535UR	SMARTnet 24x7x4 service for PIX 535-UR bundle
CON-SNTP-PIX535FO	SMARTnet 24x7x4 service for PIX 535-FO bundle
CON-S2P-PIX535	SMARTnet 24x7x2 service for PIX 535-R chassis only
CON-S2P-PIX535R	SMARTnet 24x7x2 service for PIX 535-R bundle
CON-S2P-PIX535UR	SMARTnet 24x7x2 service for PIX 535-UR bundle
CON-S2P-PIX535FO	SMARTnet 24x7x2 service for PIX 535-FO bundle
CON-OS-PIX535	SMARTnet On-Site 8x5xNBD service for PIX 535 chassis only
CON-OS-PIX535R	SMARTnet On-Site 8x5xNBD service for PIX 535-R bundle
CON-OS-PIX535UR	SMARTnet On-Site 8x5xNBD service for PIX 535-UR bundle
CON-OS-PIX535FO	SMARTnet On-Site 8x5xNBD service for PIX 535-FO bundle
CON-OSE-PIX535	SMARTnet On-Site 8x5x4 service for PIX 535 chassis only
CON-OSE-PIX535R	SMARTnet On-Site 8x5x4 service for PIX 535-R bundle
CON-OSE-PIX535UR	SMARTnet On-Site 8x5x4 service for PIX 535-UR bundle

CON-OSE-PIX535FO	SMARTnet On-Site 8x5x4 service for PIX 535-FO bundle
CON-OSP-PIX535	SMARTnet On-Site 24x7x4 service for PIX 535 chassis only
CON-OSP-PIX535R	SMARTnet On-Site 24x7x4 service for PIX 535-R bundle
CON-OSP-PIX535UR	SMARTnet On-Site 24x7x4 service for PIX 535-UR bundle
CON-OSP-PIX535FO	SMARTnet On-Site 24x7x4 service for PIX 535-FO bundle

Additional Information

For more information, please visit the following links:

Cisco PIX Security Appliance Series:

http://www.cisco.com/go/pix

Cisco PIX Device Manager:

http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixd3_ds.pdf

Cisco Secure ACS:

http://www.cisco.com/go/acs

CiscoWorks VMS, Management Center for Firewalls, Auto Update Server Software and Security Monitor:

http://www.cisco.com/go/vms

SAFE Blueprint from Cisco:

http://www.cisco.com/go/safe

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

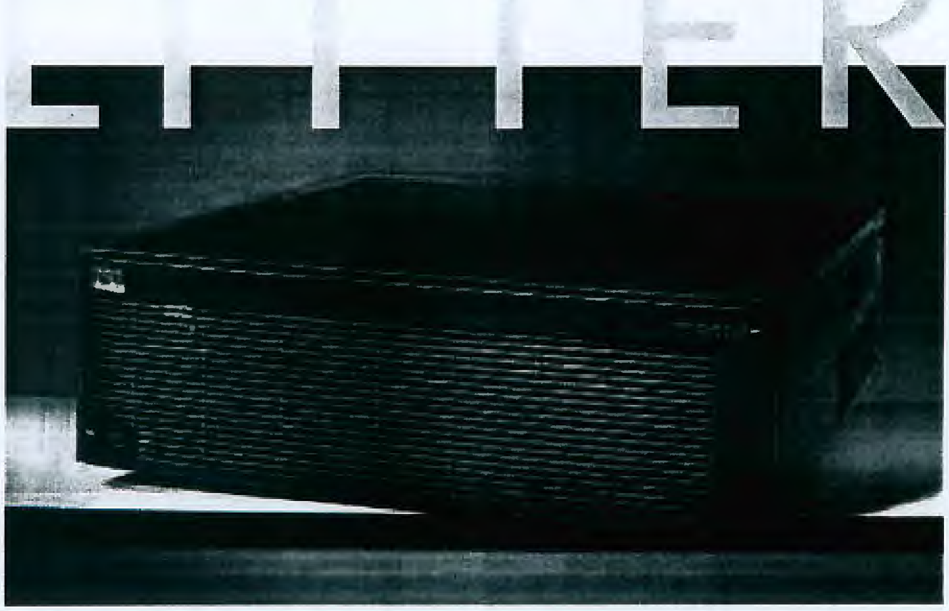
Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice FQ

PIX LITTER

New Cisco Secure PIX 535 and VPN accelerator card add higher capacity and performance to Cisco Secure PIX Firewall family



FOR PEOPLE WHO LIKE THEIR FIREWALLS BIG AND POWERFUL, WE'D like to introduce you to the Cisco Secure PIX™ 535 Firewall. Delivering carrier-class performance that meets the needs of large enterprise networks as well as service providers, the PIX 535 is definitely the pick of the litter.

The newest member of the market-leading Cisco Secure PIX Firewall family has the ability to support more than 500,000 concurrent connections and 1 Gigabit per second of throughput. With this level of performance in a single system, the PIX 535 eliminates the need to load balance multiple standalone firewalls. This capability significantly reduces network complexity without compromising security.

"The Cisco Secure PIX 535 Firewall enables an enterprise to connect to a single, fat pipe in the network that previously was a choke point for security processing," says Dennis Vogel, product manager for the Cisco Secure PIX Firewall family. "The processing power offered in a single PIX ¯35 will help enterprises keep pace with ever-growing traffic volumes while assuring reliable, consistent security protection across the network."

Playing It SAFE

The PIX 535 provides important safeguards for large corporate networks against vulnerabilities associated with doing business over the Internet. More importantly, it can be implemented as part of the recently announced Cisco SAFE blueprint for secure e-business.

Developed for real-world network deployment, Cisco SAFE helps companies compete in the Internet economy by integrating scalable, high performance security services throughout the e-business infrastructure. It takes a modular approach to security in which design, solution implementation and management processes are all provided in detail. Companies can choose from several individual modules, or "building blocks," each designed, tested and proven to address specific e-business applications, such as electronic commerce or supply chain management. (See "Play It SAFE, Sam," page 67.)

Firewall Tip: Add an IDS

Deploying an intrusion detection system (IDS) to complement your firewall can significantly enhance your security posture. A firewall's primary function is to control access to services and hosts based on your site security policy. If a connection to a specific host is permitted, the firewall may not be configured to inspect the content of the permitted traffic. For example, all connection requests to a Web server in a demilitarized zone (DMZ) may be permitted by a misconfigured firewall, including malicious traffic designed to exploit a buffer overflow vulnerability in an HTTP server. While some firewalls may not protect against data- or content-driven attacks, an IDS will. An IDS analyzes packet datastreams within a network, searching for unauthorized activity. Furthermore, firewalls typically will not protect you against attacks originating from inside your network or entering your environment from a nonfirewalled ingress point, such as a remote access server. IDS appliances can be strategically deployed to monitor activity from internal sources and other network ingress points without impacting your network performance. Today, network administrators have the choice of deploying dedicated IDS appliances such as the Cisco Secure 4210 IDS appliance and the Catalyst® 6000 IDS module, or turning on IDS capabilities inherent in Cisco IOS® routers and PIX firewalls (see "Security Blanket: Weaving Security into the Network Fabric," page 61).

Which PIX Is Right for You?

From the home office to the central office, there's a Cisco Secure PIX Firewall to meet any environment's security and virtual private network (VPN) requirements.

Cisco Secure PIX 506
Remote office or branch office
Throughput: 9 Mbps
Sessions: 1000
CPU: 200MHz
Interfaces: 2

Cisco Secure PIX 515
Small and midsized business
Throughput: 170 Mbps
Sessions: 128,000
CPU: 200MHz
Interfaces: up to 6

Reprinted with permission from *Packet*™ magazine (Volume 13, No. 1), copyright © 2001 by Cisco Systems,Inc. All rights reserved.

Well-Bred Family

The new PIX 535 extends the line of the market-leading Cisco Secure PIX Firewall family. All PIX firewalls offer built-in IP security (IPsec) encryption, allowing secure site-to-site connectivity or deployment of secure, remote-access VPNs. Like other PIX models, the PIX 535 also supports redundant units with stateful failover capabilities to ensure continued secure processing should the primary unit experience a problem.

Booster Shot—the VPN Accelerator Card

The new VPN accelerator card for the Cisco Secure PIX Firewall family improves the performance of VPNs by offloading IPsec encryption functions from the central Firewall processor to dedicated hardware. Installed in a PCI slot inside the PIX chassis, the card works transparently and does not require activation commands nor configuration changes. It is quite literally a "plug and play" process.

The VPN accelerator card encrypts data using the Data Encryption Standard (DES) and Triple DES algorithms at speeds up to 100 Mbps. By handling IPsec-related tasks such as hashing, key exchange, and storing security associations, the card frees the PIX main processor and memory for other perimeter security functions.▲▲

Fools for Security

The Motley Fool recently selected Cisco Secure PIX firewalls to secure its popular financial Web site, Fool.com. The Fool's IT department evaluated several software-based solutions, but decided against them because they were based on general-purpose operating systems. The evaluation team's preference was to go with a robust, hardened, VPN-enabled firewall appliance that wasn't as susceptible to the types of bugs, glitches and vulnerabilities often associated with other firewalls.

"Cisco's PIX is exactly what we wanted," explained Joel Salamone, MIS Director for The Motley Fool. "There is no extraneous software cluttering the operating system that can be exploited." The PIX family's similar management interface and configuration also shortened training time, and guaranteed easier administration. In addition, the number of maximum possible connections running through PIX was more than enough to accommodate the Fool's global network needs. "One of the things we really like about the PIX," said Dwight Gibbs, Chief Technology Officer for The Motley Fool, "is that it enabled us to quickly and inexpensively roll out a VPN linking our offices in the US, UK, and Germany. We can now collaborate securely thanks to the PIX."

Cisco Secure PIX 520
Enterprise
Throughput: 370 Mbps
Sessions: 250,000
CPU: 350 MHz
Interfaces: up to 6

Cisco Secure PIX 525
Large enterprise
Throughput: 370 Mbps
Sessions: 280,000
CPU: 600 MHz
Interfaces: up to 8

Cisco Secure PIX 535
Large enterprise and service provider
Throughput: 1.0 Gbps
Sessions: 500,000
CPU: 1 GHz
Interfaces: up to 8

Apêndice FR

Cisco PIX **525** Security Appliance

The Cisco PIX® 525 Security Appliance delivers enterprise-class security for medium-to-large enterprise networks in a reliable, purpose-built appliance. Its modular two-rack unit (2RU) design supports up to eight 10/100 Fast Ethernet interfaces or three Gigabit Ethernet interfaces, making it an ideal choice for businesses requiring a resilient, high performance, Gigabit Ethernet-ready solution that provides solid investment protection. Part of the world-leading Cisco PIX Security Appliance Series, the Cisco PIX 525 Security Appliance provides a wide range of rich integrated security services, hardware VPN acceleration capabilities, and powerful remote management capabilities in a cost-effective, highly-resilient solution.

Enterprise-Class Security for Medium-to-Large Enterprise Networks

The Cisco PIX 525 Security Appliance delivers a multilayered defense for large enterprise networks through rich, integrated security services including stateful inspection firewalling, protocol and application inspection, virtual private networking (VPN) in-line intrusion protection and rich multimedia and voice security in a single device. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access.

Figure 1
Cisco PIX 525 Security Appliance

Enterprise networks benefit from an additional layer of security via intelligent, "application-aware" security services that examine packet streams at Layers 4–7, using inspection engines specialized for many of today's popular applications. Administrators can also easily create custom security policies for firewall traffic by using the flexible access control methods and the more than 100 predefined applications, services, and protocols that Cisco PIX Security Appliances provide.

Market-Leading Voice-over-IP Security Services Protect Next-Generation Converged Networks

Cisco PIX Security Appliances provide market-leading protection for a wide range of voice-over-IP (VoIP) and multimedia standards, allowing businesses to securely take advantage of the many benefits that converged data, voice, and video networks deliver. By combining VPN with the rich stateful inspection firewall services that Cisco PIX Security Appliances provide for these converged networking standards, businesses can securely extend voice and multimedia services to home office and remote office environments for additional cost savings, improved productivity, and competitive advantage.

Flexible VPN Services Extend Networks Economically to Remote Networks and Mobile Users

Businesses can securely extend their networks across low-cost Internet connections to mobile users, business partners, and remote offices worldwide using the full-featured VPN capabilities provided by the Cisco PIX 525 Security Appliance. Solutions range from standards-based site-to-site VPN leveraging the Internet Key Exchange (IKE) and IP security (IPsec) VPN standards, to the innovative Cisco Easy VPN capabilities found in Cisco PIX Security Appliances and other Cisco security solutions—such as Cisco IOS® routers and Cisco VPN 3000 Series Concentrators. Easy VPN delivers a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture that eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Cisco PIX Security Appliances encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced Encryption Standard (AES) encryption. Certain Cisco PIX 525 Security Appliance models have integrated hardware VPN acceleration capabilities, delivering highly scalable, high performance VPN services.

Integrated Intrusion Protection Guards Against Popular Internet Threats

The integrated in-line intrusion-protection capabilities of the Cisco PIX 525 Security Appliance can protect enterprise networks from many popular forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Security Appliances keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time.

Award-Winning Resiliency Provides Maximum Business Uptime

Select models of Cisco PIX 525 Security Appliances provide stateful failover capabilities that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby, high-availability architecture, Cisco PIX Security Appliances that are configured as a failover pair continuously synchronize their connection state and device configuration data. Synchronization can take place over a high-speed LAN connection, providing another layer of protection through the ability to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned between appliances, with complete transparency to users.

Robust Remote-Management Solutions Lower Total Cost of Ownership

The Cisco PIX 525 Security Appliance is a reliable, easy-to-maintain platform that provides a wide variety of methods for configuring, monitoring, and troubleshooting. Management solutions range from centralized, policy-based management tools to integrated, Web-based management to support for remote monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog.

Administrators can easily manage large numbers of remote Cisco PIX Security Appliances using CiscoWorks VPN/ Security Management Solution (VMS). This suite consists of numerous modules including Management Center for Firewalls, Auto Update Server Software and Security Monitor. This powerful combination provides a highly scalable, next-generation, three-tier management solution that includes the following features:

- Comprehensive configuration and software image management
- Device hierarchy with "Smart Rules"-based configuration inheritance
- Customizable administrative roles and access privileges
- Comprehensive enterprise change management and auditing
- "Touchless" software image management for remote Cisco PIX Security Appliances
- Support for dynamically addressed appliances

Additional integrated event management and inventory solutions are also available as part of the CiscoWorks VMS network management suite.

The integrated Cisco PIX Device Manager provides an intuitive, Web-based management interface for remotely configuring, monitoring, and troubleshooting a Cisco PIX 525 Security Appliance—without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. A setup wizard is provided for easy installation into any network environment.

Alternatively, through methods including Telnet and Secure Shell (SSH), or out of band through a console port, administrators can remotely configure, monitor, and troubleshoot Cisco PIX Security Appliances using a command-line interface (CLI).

Table 1 Key Product Features and Benefits

Key Features	Benefit
Enterprise-Class Security	
True security appliance	• Uses a proprietary, hardened operating system that eliminates security risks associated with general purpose operating systems • Cisco quality and no moving parts provide a highly reliable security platform
Stateful inspection firewall	• Provides perimeter network security to prevent unauthorized network access • Uses state-of-the-art Cisco ASA for robust stateful inspection firewall services • Provides flexible access-control capabilities for over 100 predefined applications, services and protocols, with the ability to define custom applications and services • Includes numerous application-aware inspection engines that secure advanced networking protocols such as H.323 Version 4, Session Initiation Protocol (SIP), Cisco Skinny Client Control Protocol (SCCP), Real-Time Streaming Protocol (RTSP), Internet Locator Service (ILS), and more • Includes content filtering for Java and ActiveX applets
Easy VPN Server	• Provides remote access VPN concentrator services for a wide variety of Cisco software or hardware-based VPN clients • Pushes VPN policy dynamically to Cisco Easy VPN Remote-enabled solutions upon connection, ensuring the latest corporate security policies are enforced • Extends VPN reach into environments using Network Address Translation (NAT) or Port Address Translation (PAT), via support of Internet Engineering Task Force (IETF) UDP-based draft standard for NAT traversal

Table 1 Key Product Features and Benefits

Key Features	Benefit
Site-to-site VPN	• Supports IKE and IPsec VPN standards • Ensures data privacy/integrity and strong authentication to remote networks and remote users over the Internet • Supports 56-bit DES, 168-bit 3DES and up to 256-bit AES data encryption to ensure data privacy
Intrusion protection	• Provides protection from over 55 different types of popular network-based attacks ranging from malformed packet attacks to DoS attacks • Integrates with Cisco Network Intrusion Detection System (IDS) sensors for the ability to dynamically block/shun hostile network nodes via the firewall
AAA support	• Integrates with popular authentication, authorization, and accounting services via TACACS+ and RADIUS support • Provides tight integration with Cisco Secure Access Control Server (ACS)
X.509 certificate and CRL support	• Supports SCEP-based enrollment with leading X.509 solutions from Baltimore, Entrust, Microsoft, and VeriSign
Integration with leading third-party solutions	• Supports the broad range of Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions that provide URL filtering, content filtering, virus protection, scalable remote management, and more
Robust Network Services/Integration	
Virtual LAN (VLAN)-based virtual interfaces	• Provides increased flexibility when defining security policies and eases overall integration into switched network environments by supporting the creation of logical interfaces based on IEEE 802.1q VLAN tags, and the creation of security policies based on these virtual interfaces • Supports multiple virtual interfaces on a single physical interface through VLAN trunking • Supports multiple VLAN trunks per Cisco PIX Security Appliance • Supports up to 10 VLANs on Cisco PIX 525 Security Appliances
Open Shortest Path First (OSPF) dynamic routing	• Provides comprehensive OSPF dynamic routing services using technology based on world-renowned Cisco IOS Software • Offers improved network reliability through fast route convergence and secure, efficient route distribution • Delivers a secure routing solution in environments using NAT through tight integration with Cisco PIX Security Appliance NAT services • Supports MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks • Provides route redistribution between OSPF processes, including OSPF, static, and connected routes • Supports load balancing across equal-cost multipath routes
DHCP server	• Provides DHCP Server services one or more interfaces for devices to obtain IP addresses dynamically • Includes extensions for support of Cisco IP Phones and Cisco SoftPhone IP telephony solutions
DHCP relay	• Forwards DHCP requests from internal devices to an administrator-specified DHCP server, enabling centralized distribution, tracking, and maintenance of IP addresses
NAT/PAT support	• Provides rich dynamic/static NAT and PAT capabilities

Table 1 Key Product Features and Benefits

Key Features	Benefit
Rich Remote Management Options	
CiscoWorks VPN/ Security Management Solution (CiscoWorks VMS)	• Comprehensive management suite for large scale deployments • Integrates policy management, software maintenance, and security monitoring
PIX Device Manager (PDM)	• Intuitive, Web-based GUI enables simple, secure remote management of Cisco PIX Security Appliances • Provides wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events
Auto Update	• Provides "touchless" secure remote management of Cisco PIX Security Appliance configuration and software images via a unique push/pull management model • Next-generation secure XML/HTTPS management interface can be leveraged by Cisco and third-party management applications for remote Cisco PIX Security Appliance configuration management, inventory, software image management/deployment and monitoring • Integrates seamlessly with CiscoWorks Management Center for Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 Cisco PIX Security Appliances (per management server)
Cisco PIX CLI	• Allows customers to use existing PIX CLI knowledge for easy installation and management without additional training • Accessible through variety of methods including console port, Telnet, and SSH
Command-level authorization	• Enables businesses to create up to 16 customizable administrative roles/profiles for accessing Cisco PIX Security Appliances (for example, monitoring only, read-only access to configuration, VPN administrator, firewall/NAT administrator, and so on) • Leverages either the internal administrator database or outside sources via TACACS+, such as Cisco Secure ACS
SNMP and syslog support	• Provide remote monitoring and logging capabilities, with integration into Cisco and third-party management applications
Flexible Expansion Capabilities	
Fast Ethernet and Gigabit Ethernet expansion options	• Supports easy installation of additional network interfaces via 3 PCI expansion slots • Supports expansion cards including single-port Fast Ethernet card, 4-port Fast Ethernet card, and single-port Gigabit Ethernet card
Hardware VPN acceleration options	• Delivers high speed VPN services via support of VPN Accelerator Card (VAC) and VPN Accelerator Card+ (VAC+)

License Options

The Cisco PIX 525 Security Appliance is available in three primary models that provide different levels of interface density, failover capabilities, and VPN throughput.

Restricted Software License

The Cisco PIX 525 "Restricted" (PIX 525-R) model provides an excellent value for organizations looking for robust Cisco PIX Security Appliance services with Gigabit Ethernet support, medium interface density, and moderate VPN throughput requirements. It includes 128 MB of RAM and support for up to six 10/100 Fast Ethernet or three Gigabit Ethernet interfaces.

Unrestricted Software License

The PIX 525 "Unrestricted" (PIX 525-UR) model extends the capabilities of the family with support for stateful failover, additional LAN interfaces, and increased VPN throughput via integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 256 MB of RAM, and support for up to eight 10/100 Fast Ethernet or three Gigabit Ethernet interfaces. The Cisco PIX 525-UR also adds the ability to share state information with a hot-standby Cisco PIX Security Appliance for resilient network protection.

Failover Software License

The Cisco PIX 525 "Failover" (PIX 525-FO) model is designed for use in conjunction with a PIX 525-UR, providing a cost-effective, high-availability solution. It operates in hot-standby mode acting as a complete redundant system that maintains current session state information. With the same hardware configuration as the Cisco PIX 525-UR, it delivers the ultimate in high availability for a fraction of the price.

Performance Summary

Cleartext throughput: 330 Mbps

Concurrent connections: 280,000

168-bit 3DES IPsec VPN throughput: Up to 155 Mbps with VAC+ or 72 Mbps with VAC

128-bit AES IPsec VPN throughput: Up to 165 Mbps with VAC+

256-bit AES IPsec VPN throughput: Up to 170 Mbps with VAC+

Simultaneous VPN tunnels: 2000

Technical Specifications

Processor: 600-MHz Intel Pentium III Processor

Random access memory: 128 MB or 256 MB of SDRAM

Flash memory: 16 MB

Cache: 256 KB level 2 at 600 MHz

System bus: Single 32-bit, 33-MHz PCI

Environmental Operating Ranges

Operating

Temperature: –25° to 104°F (–5° to 40°C)

Relative Humidity: 5% to 95%, noncondensing

Altitude: 0 to 6500 ft (2000 m)

Shock: 1.14 m/sec (45 in./sec) 1/2 sine input

Vibration: 0.41 Grms2 (3–500 Hz) random input

Acoustic Noise: 45 dBa maximum

Nonoperating

Temperature: –13° to 158°F (–25° to 70°C)

Relative Humidity: 5% to 95%, noncondensing

Altitude: 0 to 15,000 ft (4570 m)

Shock: 30G

Vibration: 0.41 Grms2 (3–500 Hz) random input

Power

Input (per power supply)

Range Line Voltage: 100V to 240V AC or 48V DC to 60V DC

Nominal Line Voltage: 100V to 240V AC or 48V DC to 60V DC

Current: 5–2.5 Amps AC or 12 Amps DC

Frequency: 50 to 60 Hz, single phase

Output

Steady State: 50W

Maximum Peak: 65W

Maximum Heat Dissipation: 410 BTU/hr, full power usage (65W)

Physical Specifications

Dimensions and Weight Specifications

Form factor: 2 RU, standard 19-in. rack mountable

Dimensions (H x W x D): 3.5 x 17.5 x 18.25 in. (8.89 x 44.45 x 46.36 cm)

Weight (one power supply): 32 lb (14.5 kg)

Expansion

Three 32-bit/33-MHz PCI slots

Two 168-pin DIMM RAM slots, supporting up to 256 MB memory maximum

Interfaces

Console Port: RS-232 (RJ-45) 9600 baud

Failover Port: RS-232 (DB-15) 115 Kbps (Cisco specified cable required)

Two integrated 10/100 Fast Ethernet ports, auto-negotiate (half/full duplex), RJ-45

Regulatory and Standards Compliance

Safety

UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001

Electro Magnetic Compatibility (EMC)

CE marking, FCC Part 15 Class A, AS/NZS 3548 Class A, VCCI Class A, EN55022 Class A, CISPR22 Class A, EN61000-3-2, EN61000-3-3

Product Ordering Information

PIX-525	PIX 525 chassis only
PIX-525-DC	PIX 525 DC chassis only
PIX-525-R-BUN	PIX 525 restricted bundle (chassis, restricted software, 2 10/100 ports, 128 MB RAM)
PIX-525-UR-BUN	PIX 525 unrestricted bundle (chassis, unrestricted software, 2 10/100 ports, 256 MB RAM, VAC or VAC+)
PIX-525-UR-GE-BUN	PIX 525 unrestricted 2 GE + 2 FE bundle (chassis, unrestricted software, 2 Gigabit Ethernet + 2 10/100 ports, 256 MB RAM, VAC or VAC+)
PIX-525-FO-BUN	PIX 525 failover bundle (chassis, failover software, 2 10/100 ports, 256 MB RAM, VAC or VAC+)
PIX-525-FO-GE-BUN	PIX 525 failover 2 GE + 2 FE bundle (chassis, failover software, 2 Gigabit Ethernet + 2 10/100 ports, VAC or VAC+)
PIX-525-HW=	PIX 525 rack-mount kit, console cable and failover serial cable
PIX-FO=	PIX failover serial cable
PIX-4FE	4-port 10/100 Fast Ethernet PCI expansion card
PIX-1FE	Single-port 10/100 Fast Ethernet PCI expansion card
PIX-1GE-66	Single-port Gigabit Ethernet 64-bit/66-MHz PCI expansion card, Multimode (SX) SC connector
PIX-VPN-ACCEL	3DES IPsec hardware VAC
PIX-VAC-PLUS	3DES/AES IPsec hardware VAC+

PIX-VPN-3DES	168-bit 3DES and up to 256-bit AES encryption software license
PIX-VPN-3DES=	168-bit 3DES and up to 256-bit AES encryption software license
PIX-VPN-DES	56-bit DES encryption software license
PIX-VPN-DES=	56-bit DES encryption software license

Support Services

Support services are available from Cisco and Cisco partners. Cisco SMARTnet service augments customer support resources, and provides anywhere, anytime access to technical resources (both online and by telephone), the ability to download updated system software, and hardware advance replacement.

Support Ordering Information

CON-SNT-PIX525	SMARTnet 8x5xNBD service for PIX 525 chassis only
CON-SNT-PIX525R	SMARTnet 8x5xNBD service for PIX 525-R bundle
CON-SNT-PIX525UR	SMARTnet 8x5xNBD service for PIX 525-UR bundle
CON-SNT-PIX525FO	SMARTnet 8x5xNBD service for PIX 525-FO bundle
CON-SNTE-PIX525	SMARTnet 8x5x4 service for PIX 525 chassis only
CON-SNTE-PIX525R	SMARTnet 8x5x4 service for PIX 525-R bundle
CON-SNTE-PIX525UR	SMARTnet 8x5x4 service for PIX 525-UR bundle
CON-SNTE-PIX525FO	SMARTnet 8x5x4 service for PIX 525-FO bundle
CON-SNTP-PIX525	SMARTnet 24x7x4 service for PIX 525 chassis only
CON-SNTP-PIX525R	SMARTnet 24x7x4 service for PIX 525-R bundle
CON-SNTP-PIX525UR	SMARTnet 24x7x4 service for PIX 525-UR bundle
CON-SNTP-PIX525FO	SMARTnet 24x7x4 service for PIX 525-FO bundle
CON-S2P-PIX525R	SMARTnet 24x7x2 service for PIX 525-R bundle
CON-S2P-PIX525UR	SMARTnet 24x7x2 service for PIX 525-UR bundle
CON-S2P-PIX525FO	SMARTnet 24x7x2 service for PIX 525-FO bundle
CON-OS-PIX525	SMARTnet On-Site 8x5xNBD service for PIX 525 chassis only
CON-OS-PIX525R	SMARTnet On-Site 8x5xNBD service for PIX 525-R bundle
CON-OS-PIX525UR	SMARTnet On-Site 8x5xNBD service for PIX 525-UR bundle
CON-OS-PIX525FO	SMARTnet On-Site 8x5xNBD service for PIX 525-FO bundle
CON-OSE-PIX525	SMARTnet On-Site 8x5x4 service for PIX 525 chassis only
CON-OSE-PIX525R	SMARTnet On-Site 8x5x4 service for PIX 525-R bundle
CON-OSE-PIX525UR	SMARTnet On-Site 8x5x4 service for PIX 525-UR bundle

CON-OSE-PIX525FO	SMARTnet On-Site 8x5x4 service for PIX 525-FO bundle
CON-OSP-PIX525	SMARTnet On-Site 24x7x4 service for PIX 525 chassis only
CON-OSP-PIX525R	SMARTnet On-Site 24x7x4 service for PIX 525-R bundle
CON-OSP-PIX525UR	SMARTnet On-Site 24x7x4 service for PIX 525-UR bundle
CON-OSP-PIX525FO	SMARTnet On-Site 24x7x4 service for PIX 525-FO bundle

Additional Information

For more information, please visit the following links:

Cisco PIX Security Appliance Series:

http://www.cisco.com/go/pix

Cisco PIX Device Manager:

http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixd3_ds.pdf

Cisco Secure ACS:

http://www.cisco.com/go/acs

CiscoWorks VMS, Management Center for Firewalls, Auto Update Server Software and Security Monitor:

http://www.cisco.com/go/vms

SAFE Blueprint from Cisco:

http://www.cisco.com/go/safe

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice FS

CISCO SYSTEMS

Data Sheet

Cisco **PIX** Firewall Version 6.2

The world-leading Cisco PIX® Firewall Series of purpose-built security appliances provides robust, enterprise-class security services, including stateful inspection firewalling, virtual private networking (VPN), intrusion protection, and much more—in cost-effective, easy-to-deploy solutions. Ranging from compact, plug-and-play desktop firewalls for small/home offices to carrier-class gigabit firewalls for the most demanding enterprise and service-provider environments, Cisco PIX Firewalls provide robust security, performance, and reliability for network environments of all sizes.

Advanced Firewall Technologies Provide Enterprise-Class Network Security

Cisco PIX Firewalls deliver a broad range of advanced firewall services that protect enterprise networks from the threats lurking on the Internet and in today's network environments. The state-of-the-art Cisco Adaptive Security Algorithm (ASA) provides rich stateful inspection firewall services, tracking the state of all authorized network communications and preventing unauthorized network access. Cisco PIX Firewalls deliver an additional layer of security through intelligent, "application-aware" security services that examine packet streams at Layers 4 through 7, using inspection engines specialized for many of today's popular applications. Administrators can easily create custom security policies that will be enforced on network traffic traversing the firewall by leveraging more than 100 pre-defined applications, services, and protocols within Cisco PIX Firewalls, and the flexible access control capabilities that Cisco PIX Firewalls provide. Access to network resources can also be strongly authenticated via the Cisco PIX Firewall's seamless integration with enterprise databases, either directly using TACACS+/RADIUS or indirectly via Cisco Secure Access Control Server (ACS). In addition to these services, Cisco PIX Firewalls provide extensive logging, URL filtering, content filtering, and more in concert with Cisco AVVID (Architecture for Voice, Video and Integrated Data) partner solutions.

Market-Leading Voice-over-IP Security Services Protect Next-Generation Converged Networks

Cisco PIX Firewalls continue to provide market-leading protection for numerous voice-over-IP (VoIP) standards and other multimedia standards, including H.323, Session Initiation Protocol (SIP), Skinny, Real-Time Transport Protocol (RTP), Real-Time Streaming Protocol (RTSP), and Real-Time Transport Control Protocol (RTCP). This allows businesses to securely take advantage of the many benefits that converged data and voice networks provide, such as significant total cost of ownership (TCO) savings and the competitive advantages and improved productivity gained through the power of fully integrated voice, video, and data networks. By combining VPN with the rich stateful inspection firewall services that Cisco PIX Firewalls provide for these converged networking standards, businesses can easily extend voice and multimedia services to remote/satellite offices for additional bandwidth and cost savings.

Site-to-Site VPNs Extend Networks Economically to Remote Sites and Business Partners

Using the standards-based site-to-site VPN capabilities within Cisco PIX Firewalls, businesses can securely extend their network across low-cost Internet connections to business partners and remote/satellite offices worldwide. Built upon the Internet Key Exchange (IKE) and IP Security (IPSec) VPN standards, Cisco PIX Firewalls encrypt data using 56-bit Data Encryption Standard (DES) or advanced 168-bit Triple DES (3DES) encryption, ensuring that malicious individuals cannot see sensitive business data as it safely travels across the Internet. Cisco PIX Firewalls can also participate in X.509-based Public Key Infrastructures (PKI) and provide easy, automated certificate enrollment by taking advantage of the Simplified Certificate Enrollment Protocol (SCEP)—another Internet standard Cisco helped to pioneer. Certain Cisco PIX Firewall models also provide integrated hardware VPN acceleration, providing up to 100 Mbps of 3DES throughput and support for up to 2000 IKE security associations.

Easy VPN Enables Highly Scalable, Easy-to-Manage VPN Deployments

The innovative Easy VPN capabilities found in Cisco PIX Firewalls and other Cisco solutions—such as Cisco IOS® Software-based routers and Cisco VPN 3000 Series Concentrators—deliver a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture. Built upon the foundation of dynamic policy distribution and effortless provisioning, Easy VPN eliminates the operational costs associated with maintaining remote-device configurations typically required by traditional VPN solutions. Easy VPN enables Cisco customers to enjoy the numerous benefits that VPNs provide—increased employee productivity by taking advantage of high-speed broadband connectivity, and significantly reduced operational costs by eliminating expenses associated with legacy dialup architectures—without the problems commonly found with other remote-access VPN solutions.

Cisco PIX Firewalls provide robust, remote-access VPN concentrator services that enable enterprises to securely extend their network to traveling employees, teleworkers, and remote offices for "anytime, anywhere access" to vital corporate network resources. Acting as an Easy VPN Server, Cisco PIX Firewalls support the wide range of Cisco software- and hardware-based Easy VPN Remote products. By dynamically pushing VPN security policies to Easy VPN-enabled users as they connect, Cisco PIX Firewalls ensure that the latest VPN security policy is consistently enforced for all remote-access users.

Certain models of Cisco PIX Firewalls can also act as "hardware VPN clients" using the new Easy VPN Remote features in Cisco PIX Firewall OS, transparently providing secure access to a corporate network for all devices protected by a Cisco PIX Firewall in a remote network. This dramatically simplifies the initial deployment and ongoing management of VPNs deployed to remote offices and teleworker environments by eliminating the need to install and maintain VPN client software on the individual devices protected by a remote Cisco PIX Firewall. Advanced client-side resiliency features ensure maximum VPN uptime by providing automatic failover to backup Easy VPN Servers in the event of a network or service failure.

Integrated Intrusion Protection Guards from Popular Internet Threats

The integrated intrusion-protection capabilities in Cisco PIX Firewalls protect today's networks from many popular forms of attacks, including Denial-of-Service (DoS) attacks and malformed packet attacks. Using a wealth of advanced intrusion-protection features, including DNSGuard, FloodGuard, FragGuard, MailGuard, and TCP intercept, in addition to looking for more than 55 different attack "signatures," Cisco PIX Firewalls keep a vigilant watch for attacks, can optionally block them, and can notify administrators about them in real time. Additionally, Cisco PIX Firewalls support virtual packet reassembly, searching for attacks that are hidden over a series of fragmented packets. Strong integration with Cisco Intrusion Detection Systems (IDS) sensors enables Cisco PIX Firewalls to automatically shun (block) network nodes identified as being hostile by Cisco IDS sensors.

Enterprise-Class Resiliency Provides Maximum Business Uptime

Cisco PIX Firewalls provide award-winning stateful failover capabilities (on select models) that ensure resilient network protection for enterprise network environments. Employing a cost-effective, active-standby high-availability architecture, Cisco PIX Firewalls configured as a failover pair continuously synchronize connection state information and device configuration data between one another. Performing this synchronization over a high-speed LAN connection provides the added benefit of being able to geographically separate failover pair members, thus providing a further layer of protection. In the rare event of a system or network failure, network sessions are automatically transitioned between firewalls seamlessly, and with complete transparency to network users.

Robust Remote-Management Solutions Lower Total Cost of Ownership

Cisco PIX Firewalls deliver a wealth of remote-management methods for configuration, monitoring, and troubleshooting. Management solutions range from an integrated, Web-based management application to highly scalable multi-firewall management tools to support for remote-monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. Cisco PIX Firewalls additionally provide up to 16 levels of customizable administrative roles, so that enterprises can grant administrators and operations personnel the appropriate level of permissions they need for each firewall they manage (for example, monitoring only, read-only access to the configuration, VPN configuration only, firewall configuration only, etc.). Cisco PIX Firewalls now also support Auto Update, a revolutionary secure remote-management capability that ensures firewalls configurations and software images are kept up-to-date.

Cisco PIX Device Manager (PDM), integrated with Cisco PIX Firewalls, provides administrators an intuitive, Web-based management interface for remotely configuring and monitoring a single Cisco PIX Firewall, without requiring any software (other than a standard Web browser) to be installed on an administrator's computer. Administrators can also remotely configure, monitor, and troubleshoot Cisco PIX Firewalls using a command-line interface (CLI) through various methods, including Telnet and Secure Shell (SSH) Protocol, or out-of-band via a console port.

Administrators can easily manage a large number of remote Cisco PIX Firewalls using either the new combination of the CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server, or Cisco Secure Policy Manager (CSPM)—all available within the Cisco VPN Security Management Solution (VMS) network management suite. The CiscoWorks Management Center for Cisco PIX Firewalls is a highly scalable, next-generation, three-tier management solution for Cisco PIX Firewalls that includes features such as hierarchical grouping of managed firewalls, "Smart Rules" configuration inheritance, customizable administrative roles and access privileges, workflow-based enterprise change management, comprehensive support for Cisco PIX Firewall's new Auto Update capabilities, and support for dynamically addressed firewalls. Cisco Secure Policy Manager Release 3.0 is a policy-based centralized management solution for Cisco PIX Firewalls that includes a task-based interface, an interactive network topology map, policy wizards, and policy import capabilities. Additional integrated event management and inventory solutions are also available as part of the Cisco VMS network management suite.

New Features Found in Cisco PIX Firewall Release 6.2

Cisco PIX Firewall Release 6.2 provides a wealth of new innovative features, which are detailed below:

Table 1 New Features and Benefits

New Features	Benefits
Enterprise-Class Security	
LAN-based failover	• Extends failover functionality and enables geographic separation of Cisco PIX Firewalls in a failover pair by allowing failover information to be shared over a dedicated LAN connection (instead of a serial cable) between failover pairs
Bidirectional Network Address Translation (NAT)	• Enhances rich NAT functionality in Cisco PIX Firewalls to support environments with overlapping private address ranges
Turbo access control lists (ACLs)	• Provides significantly enhanced performance and deterministic search times for ACL processing; especially useful in environments where extensive ACLs are deployed
N2H2 URL filtering	• Integrates with N2H2 Sentian™ products—leading Internet filtering solutions—to provide robust employee Web access control and monitoring
Enhanced small-packet performance	• Delivers up to 48 percent more firewall performance for 64- to 512-byte packets than previous Cisco PIX Firewall OS releases, due to further optimization of small-packet processing
Management	
Auto Update	• Provides highly scalable, secure remote management of PIX Firewalls with a unique push/pull management model • Next-generation secure XML/HTTPS interface can be leveraged by Cisco and third-party management applications for remote firewall configuratio management, inventory, software image management/deployment and monitoring • Supports dynamically addressed firewalls in addition to firewalls with static IP addresses • Integrates seamlessly with CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server for robust, scalable remote management of up to 1000 PIX Firewalls
Object grouping	• Enables administrators to group network objects (such as devices, networks, and services) into logical groups to greatly simplify access control rule definition and maintenance

Table 1 New Features and Benefits

New Features	Benefits
Command-level authorization	• Enables businesses to create up to 16 customizable administrative roles and profiles for accessing Cisco PIX Firewalls (for example, monitoring only, read-only access to configuration, VPN administrator, firewall administrator, etc.) • Uses either the internal Cisco PIX Firewall administrator database or outside sources via TACACS+, such as Cisco Secure ACS
Dynamic ACLs via Cisco Secure ACS	• Supports dynamic downloading and enforcement of ACLs on a per-user basis, upon user authentication with the firewall
Network Time Protocol (NTP) v3 client	• Provides convenient method for synchronizing the clock on Cisco PIX Firewalls with other devices on a network
CPU monitoring via SNMP v2	• Extends SNMP-based remote firewall health monitoring to include the ability to monitor CPU utilization
Software and configuration updates via HTTP and HTTPS	• Adds support for downloading Cisco PIX Firewall OS and Cisco PIX Device Manager software, as well as configuration updates via HTTP or HTTPS • Provides ability to deliver configuration and software updates over authenticated, encrypted network connection
HTTPS-based CLI access	• Delivers flexible, secure interface for interactive and easily scriptable access to Cisco PIX Firewall CLI via standard HTTPS requests
Packet capture	• Gives administrators new, powerful troubleshooting capabilities by providing robust packet-capturing facilities on each interface of the firewall • Supports several methods of accessing captured packets, including via the console, secure Web access or a file exported to a Trivial File Transfer Protocol (TFTP) server
Small Office/Home Office	
Easy VPN Remote (hardware VPN client)	• Enables dramatically simplified VPN rollouts to small office, teleworker, and remote/branch-office environments, allowing Cisco PIX 501, 506, and 506E Firewalls to act as hardware VPN clients, and eliminating the provisioning complexities of traditional site-to-site VPN deployments • Downloads VPN policy dynamically from an Easy VPN Server upon connection, ensuring the latest corporate security policies are enforced • Provides robust client-side VPN resiliency with support for up to ten Easy VPN servers with automatic failover, in addition to Dead Peer Detection (DPD) support • Enables the network behind a Cisco PIX Firewall to appear as a single user to the VPN headend when using Easy VPN Remote Client Mode • Provides site-to-site VPN-like functionality without requiring any additional provisioning when using Easy VPN Remote Network Extension Mode • Supports both split and non-split tunneling environments • Provides intelligent, transparent Domain Name System (DNS) proxy capabilities for access to both corporate and public DNS servers
PPP over Ethernet (PPPoE) support	• Ensures compatibility with networks that require PPPoE support, such as xDSL and cable modem broadband environments

Table 1 New Features and Benefits

New Features	Benefits
Voice-over-IP (VoIP)/Multimedia	
Multicast support	• Supports wide range of multicast applications by introducing support for Internet Group Management Protocol (IGMP) v2 and stub multicast routing, including NAT and Port Address Translation (PAT) and the ability to build access control lists for multicast traffic
PAT for H.323 and SIP	• Extends market-leading VoIP support and enables SIP and H.323 to work in PAT environments, typically found in home offices and remote offices
DHCP server support for Cisco IP phones	• Simplifies remote Cisco IP Phone deployments by providing Cisco CallManager contact information via DHCP options 66 and 150 to Cisco IP phones for automated bootstrapping
Internet Locator Service (ILS) Fixup	• Adds support for ILS, a popular directory service used by applications suc as Microsoft NetMeeting, SiteServer and Active Directory, for registration and location of network entities/endpoints

Technical Specifications

VPN Client Compatibility

Cisco PIX Firewalls support a wide variety of software- and hardware-based VPN clients, including:

Software IPSec VPN clients	Cisco Secure VPN Client Release 1.1 Cisco VPN 3000 Concentrator Client, Release 2.5 and higher Cisco VPN Client for Microsoft Windows, Release 3.0 and higher Cisco VPN Client for Linux, Release 3.5 and higher Cisco VPN Client for Solaris, Release 3.5 and higher Cisco VPN Client for Mac OS X, Release 3.5 and higher
Hardware IPSec VPN clients	Cisco VPN 3002 Hardware Client, Release 3.0 and higher Cisco IOS Software Easy VPN Remote, Release 12.2(8)YJ Cisco PIX Firewall Easy VPN Remote, Release 6.2 and higher
Layer 2 Tunneling Protocol (L2TP)/IPSec VPN clients	Microsoft Windows 2000
Point-to-Point Tunneling Protocol (PPTP) VPN clients	Microsoft Windows 95 Microsoft Windows 98 Microsoft Windows NT 4.0 Microsoft Windows 2000

Easy VPN Server Compatibility

Cisco PIX Firewalls can now act as hardware-based VPN clients, taking advantage of the new Easy VPN Remote capabilities in Cisco PIX Firewall OS. The following Easy VPN Server platforms are supported for this deployment scenario:

Cisco IOS Routers	Release 12.2(8)T and higher
Cisco PIX Firewalls	Release 6.0(1) and higher
Cisco VPN 3000 Concentrators	Release 3.1 and higher

Cisco Site-to-Site VPN Compatibility

In addition to supporting interoperability with many third-party VPN products, Cisco PIX Firewalls interoperate with the following Cisco VPN products for site-to-site VPN connectivity:

Cisco IOS Routers	Release 12.1(6)T and higher
Cisco PIX Firewalls	Release 5.1(1) and higher
Cisco VPN 3000 Concentrators	Release 2.5.2 and higher

Cryptographic Standards Supported

Cisco PIX Firewalls support numerous cryptographic standards and related third-party products and services, including the following:

Asymmetric (public key) encryption algorithms	RSA (Rivest, Shamir, Adelman) public/private key pairs, 512 bits to 2048 bits
Symmetric encryption algorithms	DES: 56 bits 3DES: 168 bits RC4: 40, 56, 64, and 128 bits
Perfect Forward Secrecy (Diffie-Hellman key negotiation)	Group 1: 768-bits Group 2: 1024-bits
Hash algorithms	MD5: 128-bits SHA-1: 160-bits
X.509 certificate authorities	Baltimore UniCERT Entrust Authority Microsoft Windows 2000 Certificate Services VeriSign OnSite
X.509 certificate enrollment protocols	SCEP

System Requirements

Platforms supported	Cisco PIX 501 Firewall Cisco PIX 506 Firewall Cisco PIX 506E Firewall Cisco PIX 515 Firewall Cisco PIX 515E Firewall Cisco PIX 520 Firewall Cisco PIX 525 Firewall Cisco PIX 535 Firewall
RAM, minimum	32 MB, except Cisco PIX 501 which requires 16 MB
Flash memory, minimum	16 MB, except Cisco PIX 501/506/506E which require 8 MB
Expansion cards supported	Single-port 10/100 Fast Ethernet card Four-port 10/100 Fast Ethernet card Single-port Gigabit Ethernet, multimode (SX) SC, card VPN Acceleration Card (VAC)

Product Ordering Information

PIX-SW-UPGRADE=	Cisco PIX software one-time upgrade for customers without a current SMARTnet™ support contract

Support Services

Support services are available from Cisco partners as well as from Cisco. The Cisco SMARTnet service augments customer support resources. It provides 24x7x 365 access to technical resources (both online and via telephone), the ability to download updated system software, and hardware advance replacement.

Additional Information

For more information, please visit the following links:

Cisco PIX Firewall:

http://www.cisco.com/go/pix

Cisco PIX Device Manager:

http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixdm_ds.pdf

Cisco Secure ACS:

http://www.cisco.com/go/acs

Cisco Secure Policy Manager:

http://www.cisco.com/go/policymanager

Cisco VPN Security Management Solution (VMS), CiscoWorks Management Center for Cisco PIX Firewalls and Auto Update Server:

http://www.cisco.com/go/vms

Cisco SAFE Blueprint:

http://www.cisco.com/go/safe

To download the latest Cisco PIX Firewall OS and Cisco PIX Device Manager software (with a valid Cisco.com login), visit:

http://www.cisco.com/cgi-bin/tablebuild.pl/pix

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice FT

CISCO SYSTEMS

Overview

CiscoWorks Routed WAN Management Solution 1.3

The CiscoWorks Routed WAN (RWAN) Management Solution extends the CiscoWorks product family by providing a collection of powerful management applications to configure, administer, and maintain a Cisco routed wide-area network (WAN).

The RWAN solution addresses the needs of managing WANs by improving the accuracy, efficiency, and effectiveness of your network administrators and operations staff while increasing the overall availability of your network through proactive planning, deployment, and troubleshooting tools.

CiscoWorks solutions comply with Internet standards and have no network management system (NMS) prerequisites. These solutions take advantage of Web browser technologies for accessibility and integration with other third-party Web-based management tools and platforms.

Complementary CiscoWorks solutions such as the LAN Management Solution (LMS) provide a solid foundation of campus management tools. The IP Telephony Environment Monitor (ITEM) ensures the readiness and manageability of converged networks that are supporting voice over IP (VoIP) and IP telephony traffic and applications. The Cisco VPN/Security Management Solution (VMS) provides an integrated set of Web-based applications with features that assist in the deployment and monitoring of virtual private network (VPN) and security devices. Additional solutions for managing quality of service (QoS), network and user authentication, identity and access control, content networking, and Remote Monitoring (RMON) are also available.

CiscoWorks management solutions play an integral part in deploying and maintaining a Cisco AVVID (Architecture for Voice, Video and Integrated Data) network infrastructure comprising converged data, voice, and content networking.

WAN Management Challenge

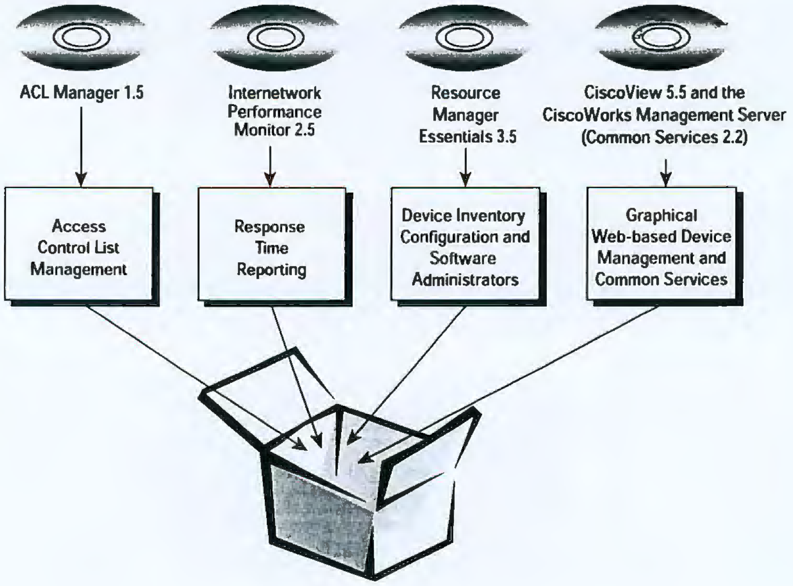
Today's enterprise WANs continue to grow as more mission-critical applications and services depend on reliable, high-performance intranet and Internet connections to remote offices, suppliers, customers, and partners worldwide. WAN links are typically the most expensive part of the network, and monitoring their performance and uptime is critical to maintaining a reliable and cost-effective network.

The ability to effectively measure response time between devices, users, and services is key to maintaining the highest levels of service quality. Proper management of WAN edge devices, links, and services becomes critical, and for this reason, Cisco has assembled a comprehensive set of WAN management tools designed to make the WAN manager's life much easier.

A Comprehensive Solution

The CiscoWorks Routed WAN Management Solution provides increased visibility into network behavior, assists in quickly troubleshooting performance bottlenecks, and provides comprehensive tools to easily administer new software and configuration changes for optimizing bandwidth and utilization across expensive and critical links in the network (Figure 1).

Figure 1
RWAN Management Solution 1.3 Components


ACL Manager 1.5
Internetwork Performance Monitor 2.5
Resource Manager Essentials 3.5
CiscoView 5.5 and the CiscoWorks Management Server (Common Services 2.2)
Access Control List Management
Response Time Reporting
Device Inventory Configuration and Software Administrators
Graphical Web-based Device Management and Common Services

Solution Components

The following applications are included in the CiscoWorks RWAN Management Solution (refer also to Table 1):

- *CiscoWorks Access Control List (ACL) Manager*—CiscoWorks ACL Manager significantly reduces the time typically required to manage and administer access control lists using the command-line interface (CLI) of Cisco IOS® Software. It provides a wizard and policy template-based approach to simplifying the setup, management, and optimization of Cisco IOS Software-based IP and Internetwork Packet Exchange (IPX) traffic filtering and device access control. This tool includes an access list editor, policy template manager, network and service class managers for scalability, access list navigation tools for troubleshooting, and automated distribution of access list updates.
- *CiscoWorks Internetwork Performance Monitor (IPM)*—CiscoWorks IPM is a network response time and availability troubleshooting application that enables WAN managers to proactively troubleshoot network response times using Cisco IOS Software embedded technology. The path and hop performance analysis provided by CiscoWorks IPM simplifies the identification of devices that are contributing to latency and network delays. CiscoWorks IPM is used to diagnose latency, identify network bottlenecks, and analyze response times. The application is also valuable for managing the effectiveness of QoS features based on IP Precedence and for troubleshooting network jitter-related problems, both of which will be needed to deploy VoIP.
- *CiscoWorks Resource Manager Essentials (RME)*— CiscoWorks RME provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis.

- *CiscoView*—CiscoView provides real-time status of Cisco devices graphically. CiscoView can drill down to display monitoring information on interfaces and access configuration functions.
- *CiscoWorks Management Server*—CiscoWorks Management Server provides the common management desktop services and security across the CiscoWorks Family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications.

Table 1 RWAN Management Solution Key Application/Function

Key Application/Function	Product	Management Benefit
ACL optimization	CiscoWorks ACL Manager	Improves router performance by organizing access filters to sort by most frequent usage patterns
ACL profiles	CiscoWorks ACL Manager	Allows administrators to quickly and uniformly apply and update template-based ACLs; can reduce WAN costs and enhance security management
ACL distribution	CiscoWorks ACL Manager	Allows administrator to automate the process of updating access list information in multiple devices
Monitoring of WAN response time characteristics	CiscoWorks IPM	Measures the responsiveness of WAN connections to determine latency and jitter, and to determine where traffic bottlenecks exist
Path and hop analysis	CiscoWorks IPM	Identifies which devices in the network are causing the greatest latency in network traffic
Detailed software and hardware inventory reporting	CiscoWorks RME	Provides accurate Cisco inventory baseline information, including memory, slots, software versions, and boot ROMs needed to make decisions about the network
Automated update engines for device software and configuration changes	CiscoWorks RME	Allows software and configuration updates to be sent to selected devices on a scheduled basis; reduces time and errors involved in network updates
Consolidated troubleshooting tools device center	CiscoWorks RME	Offers a wide collection of switch and router analysis tools accessible from a single location; device center can be linked to by third-party applications
Centralized change audit logging and application access security	CiscoWorks RME	Comprehensive change monitoring log records user and application active on the network; CiscoWorks desktop controls user access to applications, ensuring that only appropriate classes of users can access tools that change network parameters versus read-only tools
Graphic device management	CiscoView	Displays a browser representation of Cisco router and switch devices, color-coded to indicate operations states, with access to configuration and monitoring tools
Third-party integration tools (Integration utility)	CiscoWorks Management Server	Simplifies the Web integration of third-party and other Cisco management tools

Key Functions and Applications

Deployment Options

Consider the following when installing the CiscoWorks RWAN Management Solution:

- All applications do not have to be installed initially; applications not installed initially may be installed later.
- Most applications require the CiscoWorks Management Server from the Common Services CD (formerly CD One), which must be installed first.
- The CiscoWorks ACL Manager application depends on CiscoWorks RME, which is included as part of the CiscoWorks RWAN Management Solution.

All solutions can coexist on the same server if they support and operate with the services of Common Services 2.2. However, network managers may want to consider such factors as the number of applications hosted, system resources, and number of devices to be managed in determining if all or a subset of the solutions are installed on the same server.

CiscoWorks solutions offer deployment flexibility. System administrators should use the guidelines given previously when planning the deployment of the various solution bundles. Some components within a solution require the CiscoWorks Management Server and must be installed on that machine. CiscoWorks IPM and CiscoView Software can be set up on an independent server. The placement of components is a function of performance requirements and the size of the network.

Server System Requirements

Hardware/Operating System

UNIX

- System: Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) running Solaris 2.8 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM for workstations, 2-GB RAM for servers, 8-MB e-cache
- Available disk: 40-GB internal FC-AL disk drive for workstation and dual drives of this type for server configurations

Windows

- System: IBM PC compatible with 550-MHz or higher Pentium III processor running Microsoft Windows 2000 Advanced Server (with Terminal Services turned off), Server or Professional Edition with Service Pack 3 (dual processor system required for hosting multiple management solutions)
- Memory: 1-GB RAM
- Available disk: 40 GB with 2-GB swap recommended

Note: These system requirements are based on managing 500 devices with CiscoWorks RWAN and LAN Management solutions loaded on a single server. Refer to the installation documentation for more information on required operating system patches.

Client Browser System Requirements

Hardware/Operating System

UNIX

- System: Sun Ultra 10 running Solaris Versions 2.7 or 2.8
- System: HP9000 Series running HP-UX 11.0
- System: IBM RS/6000 workstation running AIX 4.3.3
- Memory: 256 MB

Windows

- System: IBM PC-compatible computer with 300-MHz or higher Pentium processor running Windows XP Professional with Service Pack 1, Windows 2000 Professional with Service Pack 2 or 3, or Windows Server with Server Pack 2 or 3.
- Memory: 256 MB

Note: Refer to the installation documentation for more information on required operating system patches.

Web Browser

UNIX

- Solaris: Netscape v4.76

Windows

- Windows 2000/XP: Netscape v4.78, 4.79
- Windows 2000/XP: Internet Explorer v6.0 or v6.0 with Service Pack1

Note: Refer to the installation documentation for more information on required operating systems patches, browser plug-ins, or Java Virtual Machine (JVM) versions.

Service and Support

CiscoWorks products are covered by the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 7 x 24 access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A Cisco SAS contract ensures that customers have easy access to the information and services needed to stay up-to-date with newly supported device packages, patches, and minor updates. For further information on service and support offerings, contact your local sales office.

Ordering Information

The CiscoWorks RWAN Management Solution includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris workstation or server. The products within this solution can be combined with other CiscoWorks products if they support the same CiscoWorks Management Server version, operating environment, and system requirements. Contact your local Cisco representative for available white papers and documentation outlining best practices for implementing a CiscoWorks management solution architecture.

To place an order, contact your Cisco sales representative.

Refer to the CiscoWorks RWAN individual product data sheets for more information on operating environment and system requirements.

For More Information

The following URL offers more information:

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps2426/index.html

Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice FU

CiscoWorks **VPN/Security Management** Solution Version 2.2

CiscoWorks VPN/Security Management Solution (VMS) is the flagship integrated security management solution from Cisco, and is an integral part of the SAFE Blueprint from Cisco for network security.

CiscoWorks VMS protects the productivity and reduces operating costs for enterprises, by combining Web-based tools for configuring, monitoring, and troubleshooting enterprise VPNs, firewalls, and network and host-based intrusion detection systems (IDS). CiscoWorks VMS delivers the industry's first robust and scalable foundation and feature set that addresses the needs of small and large-scale VPN and security deployments.

Today's business challenges and resulting security deployments require more scalability than merely supporting a large number of devices. Many customers have limited staffing, yet are asked to manage a myriad of security devices. These customers must manage the security and network infrastructure; frequently update many remote devices; implement change control and auditing when multiple organizations are involved in defining and deploying policies; enhance security without adding more headcount; or roll out remote access VPNs to all employees and monitor the VPN service.

CiscoWorks VMS enables customers to deploy security infrastructures from a small to large environment, using the following multifaceted scalability features:

- Complete SAFE Blueprint Coverage

  To completely manage a SAFE environment, a network management solution must manage SAFE infrastructure components, support features based upon an appliance or Cisco IOS® Software, and support a range of management functions. CiscoWorks VMS is uniquely able to scale across SAFE Blueprint components, including firewalls, VPNs, and network- and host-based IDSs. CiscoWorks VMS also takes advantage of Cisco Secure Access Control Server (ACS) by using a common ACS logon. CiscoWorks VMS can manage a feature set through an appliance, for example, the Cisco PIX® Firewall, or through the Cisco IOS Software. Scalable management also involves more than configuring devices. CiscoWorks VMS provides the complete range of management with features to configure, monitor, and troubleshoot the network.

- Scalable Foundation

  CiscoWorks VMS implements a foundation with a consistent user experience, which makes it easier to scale management to many devices. CiscoWorks VMS provides users with a consistent GUI, workflow, ACS logon, roles definition, platforms, database

engine, installation, and more. An industry-leading feature of this foundation is the Auto Update feature, which allows numerous devices to be updated easily and quickly. Auto Update enables devices, even remote and dynamically addressed devices, to periodically "call home" to an update server and "pull" the most current security configurations or Cisco PIX operating system. Auto Update is required to effectively scale remote office firewall deployments across intermittent links or dynamic addresses. Prior policy updating methods relied on a "push" model. Although this model works for known devices, it does not work for remote devices with unknown addresses or devices that are not always active. Without Auto Update a more manual process is required to update each remote device. The Auto Update feature provides a dramatic scalability improvement for organizations that want to deploy devices with many remote and local locations. In addition to easier and faster policy updates, Auto Update also provides consistent policy deployments.

- Enterprise Operational Integration

  CiscoWorks VMS enables organizations to easily integrate management into their operations. One operational need is to replicate policies to multiple locations. The Smart Rules hierarchy addresses this need, by enabling administrators to define device groups and implement policy inheritance. For example, an administrator can define a device group for the New York sales office and deploy that same policy to all other sales offices quic and consistently. The Command and Control Workflow feature provides change control and auditing, and is particularly important for customers who have separate groups for network and security operations. The solution includes processes for generating, approving, and deploying configurations. This can help security operations to define and approve new policies. Network operations can later deploy the new policies during their regular maintenance window. An audit of the changes can be maintained.

- Centralized Role-Based Access Control (RBAC)

  Role-based access control enables organizations to scale access privileges. CiscoWorks VMS conveniently uses a common ACS logon for users, administrators, devices, and applications. CiscoWorks VMS enables different groups to have different access rights across different devices and applications.

- Integrated Infrastructure Management

  Scalability requires that multiple components be managed, not just firewalls, but also VPNs, network- and host-based IDSs, routers, and switches. CiscoWorks VMS not only manages the security infrastructure, but also manages the network infrastructure. Customers benefit from being able to manage these components from one solution. Integrated monitoring is also required to see the larger picture. CiscoWorks VMS provides integrated monitoring of Cisco PIX and Cisco IOS syslogs, and events from network and host-based IDSs, along with event correlation.

CiscoWorks VMS Functions

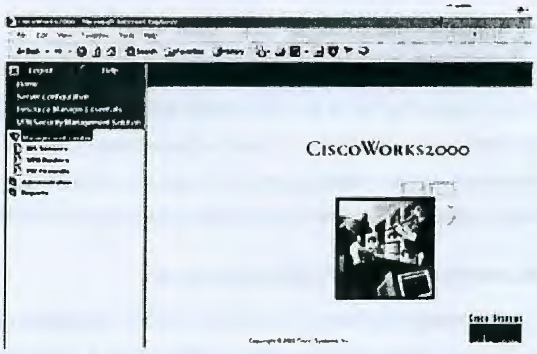
CiscoWorks VMS is launched from the CiscoWorks dashboard and is organized into several functional areas:

- Firewall management
- Auto Update Server
- IDS management, network and host-based
- VPN router management
- Security monitoring
- VPN monitoring
- Operational management

These functional areas supply multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control.

Figure 1 shows CiscoWorks VMS displayed as a "drawer" in the CiscoWorks dashboard.

Figure 1



Firewall Management

CiscoWorks VMS enables the large-scale deployment of Cisco PIX firewalls, by providing the following features:

- Smart Rules hierarchy and inheritance
- User-defined device and customer groups including nesting
- Global role-based access with administrative privileges per device and customer groups with other CiscoWorks products and Cisco Secure ACS
- Mandatory and default device settings inheritance
- Workflow deployment to device, directory, or Auto Update Server
- Look and feel of Cisco PIX Device Manager but with scalability to thousands of PIX firewalls
- Integration with other CiscoWorks network management software
- Complete SAFE Blueprint coverage for centralized management of Cisco PIX firewalls, including access control, VPN, IDS, and authentication, authorization, and accounting (AAA)

Smart Rules is an innovative feature that allows common information including access rules and settings to be inherited for all firewalls in a device or customer group. Smart Rules allows a user to define common rules once, which results in reduced configuration time, fewer administrative errors, and higher device scalability. Using Smart Rules, a user can configure a common rule such as allowing all HTTP traffic once and can apply this rule globally to all firewalls. Smart Rules can also be defined on a device or customer group basis. For specific information on the firewall management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3992/index.html

Auto Update Server for Firewall Management

CiscoWorks VMS introduces the industry's first firewall Auto Update Server that allows users to implement a "pull" model for security and Cisco PIX operating system management. Auto Update Server permits remote firewall networks with unprecedented scalability. The Auto Update Server allows Cisco PIX firewalls to both periodically and automatically contact the update server for any security configuration, Cisco PIX Operating System, and PIX Device Manager (PDM) updates. The Auto Update Server supports the following features:

- Security management of remote Cisco PIX firewalls that use Dynamic Host Control Protocol (DHCP)
- Automated Cisco PIX OS distribution to groups of Cisco PIX firewalls
- Automated Cisco PDM updates to remote firewalls
- Configuration verification at periodic intervals
- Automated replacement of inaccurate or tampered configurations
- New firewalls configured at "boot time"

The Auto Update Server is an indispensable component of any large-scale remote Cisco PIX firewall deployment. Auto Update Server is an easy-to-use solution to automatically update all remote or local firewalls with new operating system releases. Cisco is the industry's first vendor to provide this pull model of security policy and operating system management. For specific information on the Auto Update Server component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3993/index.html

Network-Based IDS Management

Administrators can use CiscoWorks VMS to configure network and switch IDS sensors. Many sensors can be quickly configured using group profiles. Additionally, a more powerful signature management feature is included to increase the accuracy and specificity of detection. Some prominent features are:

- Easy-to-use Web-based interface
- Wizards that lead users through common management tasks
- Access to the Network Security Database (NSDB), which provides meaningful information about alarms for users without IDS security expertise
- Ability to define a hierarchy of sensors containing groups and subgroups, and the ability to configure multiple sensors concurrently using group profiles
- Support for several hundred sensor deployments from each console
- Use of a robust relational database to store a high volume of data

For specific information on the network-based IDS management functionality of VMS, refer to:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

Host-Based IDS Management

CiscoWorks VMS provides threat protection for server and desktop computing systems, also known as "endpoin VMS goes beyond conventional endpoint security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown security risks that threaten enterprise networks and applications. Because CiscoWorks VMS analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs. Features of host-based IDS management include:

- Aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent.
- Provides preventive protection against entire classes of attacks including port scans, buffer overflows, Trojan horses, malformed packets, and e-mail worms.
- Offers "zero update" prevention for known and unknown attacks

- Provides industry-leading protection for UNIX and Windows servers and Windows desktops allowing customers to patch systems on their own schedules.
- Open and extensible architecture offers the capability to define and enforce security according to corporate policy.
- Scalable to thousands of agents per manager to support large enterprise deployments.

For specific information on the host-based IDS management functionality of VMS, refer to: the Management Center for Cisco Security Agents Datasheet.

VPN Router Management

CiscoWorks VMS includes functions for the setup and maintenance of large deployments of VPN connections and provides users with a point-and-click interface for setting up and deploying connections. This application is intended for scalable configuration of site-to-site VPN connections in a hub-and-spoke topology for centralized, multidevice configuration and deployment of Internet Key Exchange (IKE) and IP Security (IPsec) tunneling policies on VPN routers.

Major features include:

- Wizard-based interface for the creation of IKE and VPN tunneling policies.
- Hierarchical inheritance and Smart Rules hierarchy to reflect the organizational and common setup of devices and simplified device management
- IKE-KA (IKE Keepalive) or generic routing encapsulation (GRE) with Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) for failover routing scenarios.
- Centralized role-based access control model allows for centralized management of users and accounts.

For specific information on the VPN router management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3994/index.html

Security Monitoring

CiscoWorks VMS provides integrated monitoring to reduce the number of security monitoring consoles, reduce the number of events to monitor, and provide a broader view of security status.

- Integrated monitoring is used to capture, store, view, correlate, and report on events from many of the devices in the SAFE Blueprint such as Cisco network IDSs, switch IDSs, host IDSs, firewalls, and routers.
- Event correlation is used to identify attacks that are not easily recognizable from a single event. A flexible notification scheme and automated responses to critical events also aid in quick action.
- The event viewer can read both real-time and historical events.
- Events are color-coded and administrators can quickly isolate problems. Administrators can also define thresholds and time periods when rules can be triggered to provide notification.
- On-demand and scheduled reports facilitate ongoing monitoring.

For specific information on the security monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps3991/index.html

VPN Monitoring

CiscoWorks VMS offers a Web-based management tool that allows network administrators to collect, store, and view information on IPsec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser. This dashboard provides the following capabilities:

- Provides data on system resources related to real-time memory usage, percent CPU usage per device, and active tunnel and active sessions. This data simplifies the identification of devices with potential performance problems and devices with the highest usage.
- Enables viewing of current and long-term packet rates and packet dropped percentage which can aid in determining where excess capacity can be tapped or quickly identify bottlenecks and device throughput problems.
- Enables identification of the devices with the most persistent problems through the event log; key device and VPN statistics are evaluated against a set of global and device-specific thresholds, and exceptions are recorded in the event log.
- Provides graphing of important common metrics. Device performance comparisons provide a global view of short-term trends in VPN performance, enabling administrators to identify problem areas before they become critical failures.

For specific information on the VPN monitoring component of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2326/index.html

Operational Management

CiscoWorks VMS provides the operational management for the network, allowing network managers to perform the following:

- Quickly build a complete network inventory
- Manage device credentials information
- Monitor and report on hardware, software, configuration, and inventory changes
- Manage and deploy configuration changes and software image updates to multiple devices
- Monitor and troubleshoot critical LAN and WAN resources
- Quickly identify devices that can be used for VPNs, if upgraded with the appropriate Cisco IOS Software
- Discover which VPN devices have hardware encryption modules
- Graphically compare configurations of VPN devices
- Isolate IPsec-related problems by running customized Syslog reports

For specific information on the operational management functionality of VMS, refer to: http://www.cisco.com/en/US/products/sw/cscowork/ps2073/index.html

Server Specifications (Minimum requirements)

Server Hardware

- PC-compatible computer with 1 GHz or faster Pentium processor
- Sun UltraSPARC 60 MP with 440 MHz or faster processor
- Sun UltraSPARCIII (Sun Blade 2000 Workstation or Sun Fire280R Workgroup Server)

- CD-ROM drive
- 100BASE-T or faster connection
- 1 GB RAM
- 9 GB available disk drive space
- 2 GB virtual memory
- Color monitor with video card capable of 16-bit color

Server Operating System

CiscoWorks VMS requires the following operating systems:

- Windows 2000 Professional, Server, and Advanced Server (Service Pack 3)

Note: Support for Advanced Server requires that Terminal Services be turned off.

Sun Solaris 2.8 with patches:

109742 has been replaced by 108528-13

109322 has been replaced by 108827-15

109279 has been replaced by 108528-13

108991 has been replaced by 108827-15

Java Requirements

Sun Java plug-in 1.3.1-b24

Client Requirements

Hardware

- PC-compatible computer with 300 MHz or faster Pentium processor
- Solaris SPARCstation or Sun Ultra 10

Client Operating System

- Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP SP1 with Microsoft VM.
- Solaris 2.8

Client Browser

- Internet Explorer 6.0 Service Pack 1, on Windows operating systems
- Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition with Service Pack 3, or Windows XP; Netscape Navigator 4.76 on Solaris 2.8

The CiscoWorks Management Center for Firewalls, and CiscoWorks Management Center for VPN Routers, are supported on Internet Explorer 6.0, but not on Netscape Navigator. In addition to supporting Internet Explorer The Management Center for IDS and the Monitoring Center for Security are also supported on Netscape Navigator.

Service and Support

CiscoWorks products are eligible for coverage under the Cisco Software Application Service (SAS) program. This service program offers customers contract-based 24-hour access to the Cisco Technical Assistance Center (TAC), full Cisco.com privileges, and software maintenance updates. A SAS contract ensures that customers have easy access to the information and services needed to stay current with newly supported device packages, patches, and minor updates. For further information about service and support offerings, contact your local sales office.

Ordering Information

CiscoWorks VMS is available for purchase through regular Cisco sales and distribution channels worldwide. CiscoWorks VMS includes all the necessary components needed for an independent installation on a Microsoft Windows or Sun Solaris workstation.

For More Information

For more information, go to http://www.cisco.com/warp/public/cc/pd/wr2k/vpmnso/prodlit/ or send e-mail to ciscoworks@cisco.com

Cisco Systems

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Apêndice FV

CISCO SYSTEMS

Close Window

Toolkit: Roll over tools below

Feedback | Help

Software Advisor

HOME SOFTWARE SUPPORT FOR FEATURES SOFTWARE SUPPORT FOR HARDWARE

Search By Features | **Search By Release** | Compare Releases

Major Release	12.2T
Product Family	1751
Releases	12.2(15)T
Feature Set	IP/ADSL/VOICE PLUS IPSEC 3DES

Some features are dependent on product model, interface modules (i.e. Line Cards & Port Adapters), and/or require a software feature license.

Your selections are supported by the following

Image Name	DRAM	Flash	Product Number	Options
c1700-k9sv3y7-mz.12.2-15.T	96	16	S17C7VK9-12215T= S17C7VK9-12215T	Search For MIBs Compare Images

AAA Broadcast Accounting
AAA DNIS Map for Authorization
AAA Server Group
AAA Server Group Deadtimer
AAA Server Group Enhancements
AAA Server Groups Based on DNIS
Ability to Disable Xauth for Static IPsec Peers
Accounting of VPDN Disconnect Cause
ACL Authentication of Incoming RSH and RCP
ACL Sequence Numbering
Additional Vendor-Proprietary RADIUS Attributes
Address Resolution Protocol (ARP)
ADSL - Asymmetric Digital Subscriber Line Support
Advanced Encryption Standard (AES)
Always On Dynamic ISDN (AO/DI)
Analog DID (Direct Inward Dial)
Asynchronous Rotary Line Queuing
Asynchronous Serial Traffic Over UDP
ATM-DXI
Autoinstall Using DHCP for LAN Interfaces
Automatic modem configuration
Bandwidth Allocation Control Protocol (BACP)
BGP
BGP 4
BGP 4 Multipath Support
BGP 4 Prefix Filter and In-bound Route Maps
BGP 4 Soft Config
BGP Conditional Route Injection
BGP Hide Local-Autonomous System
BGP Hybrid CLI Support
BGP Link Bandwidth
BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN
BGP Named Community Lists
BGP Policy Accounting
BGP Prefix-Based Outbound Route Filtering
BGP Soft Reset
BRI QSIG Protocol
Call Admission Control for H.323 VoIP Gateways
Caller ID on Analog Voice Interfaces
CEF on Multipoint GRE Tunnels
CEF/dCEF - Cisco Express Forwarding

CEFv6/dCEFv6 - Cisco Express Forwarding
Certificate Auto-Enrollment
Certificate Enrollment Enhancements
Certificate Security Attribute-Based Access Control
Certification Authority Interoperability (CA)
CGMP - Cisco Group Management Protocol
Challege Handshake Authentication Protocol (CHAP)
Channelized E1 Signaling
Circuit Interface Identification Persistence for SNMP
Cisco Discovery Protocol (CDP)
Cisco Discovery Protocol (CDP) - IPv6 Address Family Support for Neighbor I...
Cisco Discovery Protocol (CDP) over ATM
Class Based Weighted Fair Queuing (CBWFQ)
Class-Based Packet Marking
CLI String Search
CNS Agents SSL Security
CNS Configuration Agent
CNS Event Agent
CNS Flow-Through Provisioning
Commented IP Access List Entries
Committed Access Rate (CAR)
Compression Control Protocol
CT1/RBS (Robbed Bit Signaling)
CUG Selection Facility Suppress Option
Custom Queueing (CQ)
Customer Profile Idle Timer Enhancements for Interesting Traffic
Default Passive Interface
DF Bit Override Functionality with IPSec Tunnels
DHCP Accounting
DHCP Client
DHCP Client - Dynamic Subnet Allocation API
DHCP Client on WAN Interfaces
DHCP ODAP Server Support
DHCP On Demand Address Pool (ODAP) Manager for non-MPLS VPN pools
DHCP Proxy Client
DHCP Relay Agent Support for Unnumbered Interfaces
DHCP Secured IP Address Assignment
DHCP Server - On Demand Address Pool Manager
DHCP Server - Option to Ignore all BOOTP Requests
DHCP Server Options - Import and Autoconfiguration
DHCP Server-Easy IP Phase 2
Dial backup
Dial Peer Enhancements
Dial-on-demand
Dialer Idle Timer Inbound Traffic Configuration
Dialer Persistent
Dialer profiles
Dialer Watch
Dialer Watch Connect Delay
Differentiated Services
Diffserv Compliant WRED
Distinguished Name Based Crypto Maps
D[illegible] Enhancements: PGM RFC-3208 Compliance
DNS-based X.25 routing
DNS Lookups over an IPv6 Transport
Double Authentication
Dynamic Multiple Encapsulation for Dial-in over ISDN
Dynamic Multipoint VPN (DMVPN)
E1 R2 Signaling
Easy IP (Phase 1)
Easy VPN Remote
Easy VPN Remote : Multiple Inside Interface Enhancements
Easy VPN Remote Enhancements
Easy VPN Remote: Local-Address Support
Easy VPN Remote: Manual Tunnel Control Enhancement
Easy VPN Server
Encrypted Vendor Specific Attributes
Enhanced IGRP (EIGRP)
Enhanced IGRP Stub Routing
Enhanced ITU-T G.168 Echo Cancellation
Enhanced Local Management Interface (ELMI)
Enhanced Password Security
Enhanced Tracking Support.
Exporting and Importing RSA Keys
Fast Fragmentation (Fast-Switched Fragmented IP Packets)

Fast-Switched Policy Routing
Flow-Based WRED
Frame Relay
Frame Relay Encapsulation
Frame Relay End-to-End Keepalive
Frame Relay Fragmentation (FRF.12)
Frame Relay FRF.9 Payload Compression
Frame Relay PVC Interface Priority Queueing
Frame Relay Router ForeSight
Frame Relay SVC Support (DTE)
Frame Relay Switching
Frame Relay Switching Diagnostics and Troubleshooting
Frame Relay Switching Enhancements: Shaping and Policing
Frame Relay Traffic Shaping (FRTS)
Frame Relay Voice Adaptive Traffic Shaping
FXO Answer and Disconnect Supervision
G.SHDSL Symmetric DSL Support
Gatekeeper Ecosystem Interoperability
Generic Routing Encapsulation (GRE)
Generic Routing Encapsulation (GRE) Tunnel Keepalive
Generic Traffic Shaping (GTS)
GLBP: Gateway Load Balancing Protocol
H.323 Call Redirection Enhancements
H.323 Scalability and Interoperability Enhancements for Gateways
Half bridge/half router for CPP and PPP
Hoot and Holler over IP
HSRP - Hot Standby Router Protocol
HSRP - Hot Standby Router Protocol and IPSec
HSRP support for ICMP Redirects
HTTP 1.1 Web Server
HTTPS - HTTP with SSL 3.0
iBGP Multipath Load Sharing
IEEE 802.1p Support
IEEE 802.1Q VLAN Support
IGMP Version 3
IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels
IKE - Initiate Aggressive Mode
IKE Extended Authentication (Xauth)
IKE Mode Configuration
IKE Security Protocol
IKE Shared Secret Using AAA Server
Integrated routing and bridging (IRB)
Interface Alias Long Name Support
Interface Index Display
Interface Range Specification
IP Enhanced IGRP Route Authentication
IP Header Compression Enhancement - PPPoATM and PPPoFR Support
IP Multicast Load Splitting across Equal-Cost Paths
IP Named Access Control List
IP Precedence for GRE Tunnels
IP Routing
IP RTP Priority
IP Summary Address for RIPv2
IP to ATM CoS, per-VC WFQ and CBWFQ
IP-to-ATM CoS
IPSec MIB Support for Cisco IPSec VPN Management
IPsec NAT Transparency
IPSec Network Security
IPSec Through Network Address Translation Support
IPSec Triple DES Encryption (3DES)
IPSec VPN High Availability Enhancements
IPv6 Extended Access Control List
IPv6 for Cisco IOS Software
ISDN
ISDN Advice of Charge (AOC)
ISDN Caller ID Callback
ISDN Cause Code Override
ISDN Leased Line at 128kbps
L2TP Dial-Out
L2TP Layer 2 Tunneling Protocol
L2TP Security
L2TP Tunnel Preservation of IP TOS
Layer 2 Forwarding-Fast Switching
Lock and Key
Low Latency Queueing (LLQ)

Low Latency Queueing (LLQ) for Frame Relay
Low Latency Queueing (LLQ) with Priority Percentage Support
Manual certificate enrollment (TFTP and cut-and-paste)
MD5 File Validation
Message Banners for AAA Authentication
Microsoft Point-to-Point Compression (MPPC)
MLPPP with Link Fragmentation Interleave (LFI)
Modem User Interface Option
Modular QoS CLI (MQC)
Modular QoS CLI (MQC) - Based Frame Relay Traffic Shaping
Modular QoS CLI (MQC) Three-Level Hierarchical Policer
MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE...
MS Callback
MS-CHAP Version 1
Multicast NAT
Multicast Source Discovery Protocol (MSDP)
Multilink PPP
Multiple RSA Keypair Support
Named Method Lists for AAA Authorization and Accounting
NAT Default Inside Server Enhancement
NAT Stateful Fail-over of Network Address Translation
NAT-Network Address Translation
NAT-Support for NetMeeting Directory (Internet Locator Service - ILS)
NAT-Support of H.323v2 RAS
NAT-Support of IP Phone to Cisco Call Manager
NBAR - Network-based Application Recognition
NBAR Real-time Transport Protocol Payload Classification
Netflow
NetFlow Aggregation
NetFlow Multiple Export Destinations
NetFlow Policy Routing (NPR)
NetFlow ToS-Based Router Aggregation
Network Time Protocol (NTP)
Next Hop Resolution Protocol (NHRP)
On Demand Routing (ODR)
OSPF
OSPF ABR type 3 LSA Filtering
OSPF Flooding Reduction
OSPF Not-So-Stubby Areas (NSSA)
OSPF On Demand Circuit (RFC 1793)
OSPF Packet Pacing
OSPF Sham-Link Support for MPLS VPN
OSPF Stub Router Advertisement
OSPF Support for Multi-VRF on CE Routers
PAD Subaddressing
Parse Bookmarks
Parser Cache
Password Authentication Protocol (PAP)
Per-User Configuration
Percentage-Based Policing and Shaping
PGM Router Assist
PIM Dense Mode State Refresh
PIM MIB Extension for IP Multicast
PIM Multicast Scalability
PIM Version 1
PIM Version 2
Policy-Based Routing (PBR)
PPP
PPP over ATM
PPP over ATM (IETF-Compliant)
PPP over Frame Relay
PPPoE Client
PPPoE on Ethernet
Pre-fragmentation For Ipsec VPNs
PRI QSIG protocol
Priority Queueing (PQ)
Privilege Command Enhancement
QoS Device Manager (QDM)
QoS for Virtual Private Networks
QoS Packet Marking
QoS Priority Percentage CLI Support
RADIUS
RADIUS Attribute 44 (Accounting Session ID) in Access Requests
RADIUS Attribute 82: Tunnel Assignment Id
RADIUS Centralized Filter Management

RADIUS for Multiple User Datagram Protocol Ports
RADIUS Route Download
RADIUS Tunnel Preference for Load Balancing and Fail-over
Random Early Detection (RED)
Rate Queues for SVC's per sub-interface
Reflexive Access Lists
Response Time Reporter (RTR)
Response Time Reporter (RTR) enhancements
Reverse Path Forwarding - Source Exists only
Reverse Route Injection (RRI)
RIP
RMON events and alarms
Rotating Through Dial Strings
RSVP - Resource Reservation Protocol
RSVP Local Policy Support
RSVP Support for Frame Relay
RSVP support for LLQ
RTP Header Compression
Secure Copy (SCP)
Secure Shell SSH Support over IPv6
Secure Shell SSH Terminal-line access
Secure Shell SSH Version 1 Integrated Client
Secure Shell SSH Version 1 Server Support
Service Assurance Agent (SAA) APM Application Performance Monitor
Service Assurance Agent (SAA) DHCP Operation
Service Assurance Agent (SAA) Distribution of Data
Service Assurance Agent (SAA) DLSW Operation
Service Assurance Agent (SAA) DNS Operation
Service Assurance Agent (SAA) Frame Relay Operation
Service Assurance Agent (SAA) FTP Operation
Service Assurance Agent (SAA) History Statistics
Service Assurance Agent (SAA) HTTP Operation
Service Assurance Agent (SAA) ICMP Echo Operation
Service Assurance Agent (SAA) ICMP Path Echo Operation
Service Assurance Agent (SAA) Jitter Operation
Service Assurance Agent (SAA) MPLS VPN Operation
Service Assurance Agent (SAA) One Way Jitter
Service Assurance Agent (SAA) Path Jitter
Service Assurance Agent (SAA) Reaction Threshold
Service Assurance Agent (SAA) Scheduling Operation
Service Assurance Agent (SAA) SNA LU2 Echo
Service Assurance Agent (SAA) SNMP Support
Service Assurance Agent (SAA) TCP Connect Operation
Service Assurance Agent (SAA) UDP Echo Operation
Show Command Redirect
Simple Network Time Protocol (SNTP)
Single Rate 3-Color Marker for Traffic Policing
Snapshot routing
SNMP (Simple Network Management Protocol)
SNMP Inform Request
SNMP Manager
SNMP Support for IOS vLAN Subinterfaces
SNMP Support for vLAN (ISL, DOT1Q) Subinterfaces
SNMP Support over VPN
SNMPv2C
Source Interface Selection for Outgoing Traffic with Certificate Authority ...
Spanning Tree Protocol (STP)
Spanning Tree Protocol (STP) Extension
Standard IP Access List Logging
Static Cache Entry for IPv6 Neighbor Discovery
Stub IP Multicast Routing
Subnetwork Bandwidth Manager (SBM)
Switched Multimegabit Data Service (SMDS)
T.38 Fax Relay for VoIP H.323
T1 Channel Associated Signaling (CAS)
T1/E1 Voice PRI Q.931
Tacacs SENDAUTH function
Tacacs Single Connection
TACACS+
TCP Window Scaling
Time-Based Access Lists Using Time Ranges
Timer and Retry Enhancements for L2TP and L2F
Traffic Policing
Transparent Bridging
Triggered RIP

Trusted Root Certification Authority
Trustpoint CLI
Tunnel Endpoint Discovery
Tunnel Type of Service (TOS)
Turbo Flooding of UDP Datagrams
UDLR Tunnel ARP and IGMP Proxy
UDP forwarding support of IP Redundancy Virtual Router Group (VRG)
Uni-Directional Link Routing (UDLR)
Unicast Reverse Path Forwarding (uRPF)
User Maximum Links
Virtual Interface Template Service
Virtual Private Dial-up Network (VPDN)
Virtual Profiles
Virtual Router Redundancy Protocol (VRRP)
Voice Call Tuning
Voice DSP Control Message Logger
Voice over Frame Relay (FRF.11)
Voice Over IP
VoIP Call Admission Control using RSVP
VoIP Outgoing Trunk Group Identification and Carrier ID for Gateways
VPDN Group Session Limiting
VPN Device Manager (VDM)
VPN Tunnel Management
WCCP Redirection on Inbound Interfaces
WCCP Version 1
WCCP Version 2
Weighted Fair Queueing (WFQ)
Weighted RED (WRED)
Wildcard Pre-Shared Key
WRED Enhancement - Explicit Congestion Notification (ECN)
x Digital Subscriber Line (xDSL) Bridge Support
X.25
X.25 Closed User Group
X.25 Failover
X.25 Load Balancing
X.25 on ISDN D-Channel
X.25 over Frame Relay (Annex G)
X.25 over TCP (XOT)
X.25 Over TCP Profiles
X.25 Remote Failure Detection
X.25 Suppression of Security Signaling Facilities
X.25 Switch Local Acknowledgement
X.25 Switching between PVCs and SVCs
X.25 Terminal Line Security for PAD Connections
X.28 Emulation

To find out more about your selected release, you can use the Bug Toolkit

Close Window

Apêndice FX

New and Changed Information

The following is a list of the new features that are supported in Cisco IOS Release 12.2 T. For additional information regarding the features supported in Cisco IOS Release 12.2 T, refer to the new feature documentation at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/index.htm

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for the new features listed in Cisco IOS Release 12.2 T, access Cisco Feature Navigator. Cisco Feature Navigator is regularly updated as new platform support is added for features.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Note MPLS Class of Service is now referred to as MPLS Quality of Service. This transition reflects the growth of MPLS to encompass a wider meaning and highlight the path toward *Any Transport over MPLS.*

New Hardware Features Supported in Cisco IOS Release 12.2(15)T

The following new hardware features are supported in Cisco IOS Release 12.2(15)T. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

1 Port Enhanced ATM Port Adapter with Support for 8K VCs

The PA-A6 is a series of single-width, single-port, ATM port adapters for Cisco 7200 series and Cisco 7401ASR routers. With advanced ATM features, the PA-A6 supports broadband aggregation, WAN aggregation, and campus/MAN aggregation.

1 and 2-port T1/E1 Multiflex Voice/WAN Interface Card

1- and 2-port T1/E1 Multiflex Voice/WAN interface cards provide basic structured and unstructured service for T1 or E1 networks. The card provides fractional data service and channelized voice services and TDM drop and insert (voice/data integration) services.

1- and 2-Port V.90 Modem WICs for Cisco 1720, 1751 and 1760 Routers

The one- and two-port V.90 Modem WICs expand the extensive range of WICs currently available on these routers. The modem WIC cards provide cost-effective basic telephone service connectivity to allow remote router management, asynchronous Dial-on-Demand routing (DDR) and dial back-up, and low-density remote access server (RAS) services.

Catalyst 4500 Access Gateway Module 16-port RJ21 FXS Module (WS-U4604-16FXS)

The 16-Port RJ21 FXS module for the Catalyst 4500 Access Gateway Module is a high density analog phone and fax interface. By providing service to analog phones and fax machines, the sixteen Foreign Exchange Station (FXS) ports emulate a PSTN central office (CO) or PBX.

Catalyst 4500 AGM Voice/WAN Bundle (WS-X4604-VOICE)

The Cisco Catalyst 4500 AGM Voice/WAN bundle provides integrated telephony and routing services to the Cisco Catalyst 4000 series and Cisco Catalyst 4500 series switches. The Cisco Catalyst 4500 AGM Voice/WAN bundle consists of the following products:

- Cisco Catalyst 4500 Access Gateway Module (WS-X4604-GWY)
- Cisco Catalyst 4500 AGM 96-channel Digital Signal Processor Set (4x6 DSP SIMMS) (WS-X4604-DSP)
- Cisco Catalyst 4500 AGM 128MB RAM DIMM (MEM-C4K-AGM128M)

Gigabit Ethernet Network Module

The Gigabit Ethernet (GE) network module provides gigabit connectivity. The throughput of the interface depends on the platform. The network module has one GBIC slot to carry any standard copper or optical Cisco GBIC, including CWDM. The GE network module optimizes the performance for branch office customers by offering a high-speed uplink to both existing and new LAN or WAN environments. The extended reach of the provided fiber connectivity allows customers the option of interconnecting branch offices with Gigabit Ethernet and avoids expensive leased serial lines. Metro area service providers now have additional options when connecting their customers in branch offices to MANs.

The Gigabit Ethernet network module is supported on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.

MRP300

The Multiservice Route Processor 300 (MRP300) is a voice-and-data-capable router that can carry voice traffic over an IP network and that can link small-to-medium-size remote Ethernet LANs to central offices over WAN links. The MRP300 has a slot for expanding flash memory; two slots that support WICs, VWICs, and VICs; two PVDM slots for adding DSPs; and a DIMM slot for upgrading DRAM.

MRP3-8FXS

The MRP3-8FXS contains an 8-port Foreign Exchange Station (FXS) module and a slot for any VIC, WIC, or VWIC module that supports digital and analog voice trunks and WAN routing interfaces. The MRP3-8FXS is similar to the analog station interface 81 card (ASI81), with the exception that the ASI81 does not have onboard Flash memory.

MRP3-16FXS

The MRP3-16FXS contains a 16-port Foreign Exchange Station (FXS) module. The MRP3-16FXS is similar to the analog station interface 161 card (ASI160), except that the ASI160 does not have onboard Flash memory.

NPE-G1

The NPE-G1 is the first network processing engine for the Cisco 7200 VXR routers to provide the functionality of both a network processing engine and an I/O controller. If used without an I/O controller, an I/O blank panel must be in place.

Although its design provides I/O controller functionality, it can also work with any I/O controller supported in the Cisco 7200 VXR routers. The NPE-G1, when installed with an I/O controller, provides the primary input/out functionality; that is, the NPE-G1 input/out functionality enhances that of the existing I/O controller. However, when both the I/O controller and NPE-G1 are present, the functionality of the auxiliary port and console port are on the I/O controller.

The NPE-G1 maintains and executes the system management functions for the Cisco 7200 VXR routers and also holds the system memory and environmental monitoring functions.

The NPE-G1 consists of one board with multiple interfaces. It is keyed so that it can be used only in the Cisco 7200 VXR routers.

RPM-XF Card for the MGX 8850

The RPM-XF card is a next-generation, high-performance model of the RPM for the MGX 8850 platform, using PXM45 processor modules. It is a router module based on an RM7000A MIPS processing engine.

The RPM-XF hardware provides forwarding technology for packet switching capabilities in excess of 2-million pps. The forwarding engine is packet based and is interfaced to the midplane of the system through a combination of switch interface technologies.

SDH/STM-1 Trunk Card for Cisco AS5850 Universal Gateway

Channelized STM-1 provides a high speed remote access aggregation solution with 63 E1s and 1890 DSO channels. The SDH/STM-1 trunk card is a high density mux/demux card that takes in an STM-1 (SDH) pipe, used to transport up to 1890 DS0 channels. The SDH/STM-1 trunk card provides an ingress connection between the Cisco AS5850 universal gateway and external networks. The SDH/STM-1 trunk card has a 155-mbps channelized SDH physical interface in a standard dial feature card (DFC) format. The SDH interface supports channelization to 64 kbps and connects to single mode fiber optic supporting intermediate reach PPP applications.

New Software Features in Cisco IOS Release 12.2(15)T

The following new features are supported in Cisco IOS Release 12.2(15)T. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

ADSL over ISDN

Cisco 826 routers connect corporate telecommuters and small offices via Internet service providers (ISPs) over asymmetric digital subscriber lines (ADSLs) to corporate LANs and the Internet. The router can provide bridging and multiprotocol routing between LAN and WAN ports. Cisco 826 routers provide connectivity to an ISDN network through an ADSL port.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco 820, Cisco SOHO 70, Cisco SOHO 76, Cisco SOHO 77, and Cisco SOHO 77H platforms.

Any Transport over MPLS (AToM)

Any Transport over MPLS (AToM) transports Layer 2 packets over a Multiprotocol Label Switching (MPLS) backbone. AToM enables service providers to connect customer sites with existing data link layer (Layer 2) networks, by using a single, integrated, packet-based network infrastructure—a Cisco MPLS network. Instead of separate networks with network management environments, service providers can deliver Layer 2 connections over an MPLS backbone. AToM provides a common framework to encapsulate and transport supported Layer 2 traffic types over an MPLS network core. AToM supports the following transport types:

- ATM AAL5 over MPLS
- ATM Cell Relay over MPLS
- Ethernet over MPLS
- Frame Relay over MPLS
- PPP over MPLS
- HDLC over MPLS

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/atomt/index.htm

ARP Optimization

The Address Resolution Protocol (ARP) is used to map a Layer 3 IP address to a Layer 2 MAC address. A Cisco router stores this mapped information in an ARP table. The ARP table provides MAC rewrite information when the router is forwarding a packet using Cisco Express Forwarding (CEF) or other IP switching technologies.

In previous versions of Cisco IOS software, the ARP table was organized for easy searching on an entry based on the IP address. However, there are cases such as interface flapping on the router and a topology change in the network in which all related ARP entries need to be refreshed for correct forwarding. This situation could consume a significant amount of CPU time in the ARP process to search and clean up all the entries. The ARP Optimization feature improves ARP performance by reducing the ARP searching time by using an improved data structure.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/arpoptim.htm

Asynchronous Call Queueing by Role

The Asynchronous Call Queueing by Role feature allows priority users who are making Telnet connection requests to busy asynchronous rotary groups to be placed at the head of the queue when asynchronous rotary line queueing is enabled. If a second priority user makes a Telnet connection request, this user will be placed behind the first priority user at the head of the queue. This feature allows a priority user to access the first available line. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftasyncq.htm

AutoQoS - VoIP

The AutoQoS - VoIP feature allows you to automate the delivery of quality of service (QoS) on your network, and provides a means for simplifying the implementation and provisioning of QoS for voice over IP (VoIP) traffic. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftautoq1.htm

BGP Hybrid CLI Support

The BGP Hybrid CLI Support feature allows the network operator to configure the Border Gateway Protocol (BGP) using the Network Layer Reachability Information (NLRI) format for IPv4 unicast commands and the address-family identifier (AFI) format for address family commands, such as IPv6, VPNv4, and Connectionless Network Service (CLNS) protocol commands. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbhycli.htm

BGP Increased Support of Numbered AS-Path Access Lists to 500

The BGP Increased Support of Numbered AS-Path Access Lists to 500 feature is an enhancement for Border Gateway Protocol (BGP) autonomous system access lists. This enhancement increases the maximum number autonomous system access lists from 199 to 500. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftiaaspa.htm

BGP Nonstop Forwarding (NSF) Awareness

Nonstop Forwarding (NSF) awareness allows a router to assist NSF-capable neighbors to continue forwarding packets during a switchover operation or during a well-known failure condition. The BGP Nonstop Forwarding Awareness feature allows an NSF-aware router that is running BGP to forward packets along routes that are already known for a router that is performing a switchover operation or is in a well-known failure mode. This capability allows the BGP peers of the failing router to retain the routing information that is advertised by the failing router and continue to use this information until the failed router has returned to normal operating behavior and is able to exchange routing information. The peering session is maintained throughout the entire NSF operation.

Cisco Nonstop Forwarding (NSF) works with the Stateful Switchover (SSO) feature in Cisco IOS software. SSO is a prerequisite of Cisco NSF. NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of Cisco NSF is to continue forwarding IP packets following a Route Processor (RP) switchover. NSF/SSO is configured in the core of your network, and NSF awareness is configured on iBGP peers in the core and the edge of the network.

BGP Restart Session After Max-Prefix Limit

The BGP Restart Session After Max-Prefix Limit feature enhances the capabilities of the **neighbor maximum-prefix** command with the introduction of the **restart** keyword. This enhancement allows the network operator to configure the time interval at which a peering session is reestablished by a router when the number of prefixes that have been received from a peer has exceeded the maximum prefix limit. The **restart** keyword has a configurable timer argument that is specified in minutes. The time range of the timer argument is from 1 to 65535. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbrsamp.htm

BGP Route-Map Policy List Support

The BGP Route-Map Policy List Support feature introduces new functionality to Border Gateway Protocol (BGP) route maps. This feature adds the capability for a network operator to group route-map match clauses into a named list called a policy list. A policy list functions like a macro within a route map. When the policy list is referenced within a route map with the **match policy-list** command, all match statements in the policy list are executed. Policy lists can be used for all applications of a route map and for redistribution between routing protocols. Policy lists can coexist with configured match and set clauses within the same subblock. Policy lists, however, do not support set statements, and policy lists are not supported by IP routing policy. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbgprpl.htm

BRI QSIG Protocol

BRI QSIG is the QSIG support over BRI interface. QSIG protocol support allows Cisco voice gateways to connect PBXs, key telephone systems (KTS), and central office switches that communicate by using the QSIG protocol.

Certificate Security Attribute-Based Access Control

Under the IP Security (IPSec) protocol, certification authority (CA) interoperability permits Cisco IOS devices and a CA to communicate so that the Cisco IOS device can obtain and use digital certificates from the CA. Certificates contain several fields that are used to determine whether a device or user is authorized to perform a specified action. The Certificate Security Attribute-Based Access Control feature adds fields to the certificate that allow specifying an access control list (ACL) to create a certificate-based ACL. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftcrtacl.htm

Cisco Easy VPN Remote Enhancements

The Cisco Easy VPN Remote Enhancements feature improve the capabilities of the Cisco Easy VPN Client feature first delivered in Cisco IOS Release 12.2(4)YA. Additional capabilities include the following:

- Establishes and terminates the IP Security (IPSec) Virtual Private Network (VPN) tunnel on demand.
- Configures up to three inside interfaces and four outside tunnels for outside interfaces on the VPN client.
- Restores the Network Address Translation (NAT) configuration automatically when the IPSec VPN tunnel is disconnected.
- Supports a **local-address** attribute that specifies which interface is used to source the Easy VPN tunnel traffic.
- Supports the **loopback** interface for Cisco uBR905 and Cisco uBR925 cable access routers with the **cable-modem dhcp-proxy interface** command.
- Enhances Peer Hostname.
- Supports Proxy DNS Server.
- Supports Cisco PIX Firewall Version 6.2 and Cisco IOS Firewall configurations on all platforms.
- Supports Simultaneous Easy VPN Client and Cisco Easy VPN Server on the same Cisco 1700 series routers.
- Uses a built-in web interface to manage the Cisco Easy VPN Remote feature on the Cisco uBR905 and Cisco uBR925 cable access routers.

These enhancement were introduced in Cisco IOS Release 12.2(8)YJ to support Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. This release is adding support for Cisco 2600, Cisco 3600, and Cisco 3700 series routers. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftezvpnr.htm

Cisco IOS Firewall Stateful Inspection of ICMP

The Cisco IOS Firewall Stateful Inspection of ICMP feature addresses the limitation of qualifying Internet Control Management Protocol (ICMP) messages into either a malicious or benign category by allowing the Cisco IOS firewall to use stateful inspection to "trust" ICMP messages that are generated within a private network and to permit the associated ICMP replies. Thus, network administrators can debug network issues without needing to block ICMP messages from entering the network because of possible intruders.

Cisco IOS Firewall Support for SIP

The Cisco IOS Firewall Support for SIP feature integrates Cisco IOS firewalls, the Voice over IP (VoIP) protocol, and Session Initiation Protocol (SIP) within a Cisco IOS based platform, enabling better network convergence.

Cisco IOS Firewall Websense URL Filtering

The Cisco IOS Firewall Websense URL Filtering feature enables your Cisco IOS firewall (also known as Cisco Secure Integrated Software [CSIS]) to interact with the Websense URL filtering software, thereby allowing you to prevent users from accessing specified websites on the basis of some policy. The Cisco IOS Firewall feature works with the Websense server to know whether a particular URL should be allowed or denied (blocked). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122yu11/ftwebsen.htm

Cisco IOS Software Feature Removal—Phase II

The Cisco IOS Software Feature Removal feature is an engineering project to permanently remove selected legacy features (or components) from the Cisco IOS code. These features will not be available in future releases of Cisco IOS software. The legacy features that have been removed as of Cisco IOS Release 12.2(15)T are as follows:

- LAN Extension
- Netware Asynchronous Services Interface (NASI)
- XRemote

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

Cisco IOS Telephony Service Version 2.1

Cisco IOS Telephony Service (ITS) offers an entry-level IP telephony solution integrated directly into Cisco IOS software. Customers can now deploy voice, data, and IP telephony on a single platform for their small offices. ITS offers a core set of phone features that customers commonly require for their everyday business needs, and leverages the wide array of voice capabilities that are available in Cisco IOS software to provide a very robust IP telephony offering for the small office environment.

Cisco ITS version 2.1 provides support for the following new features:

- additional languages
- phone loads for Cisco CallManager 3.1 and above
- GUI customization capability
- Live Feed Music on Hold (MOH)
- H450.2 and H450.3 support in Cisco IOS software
- Consultative Transfer
- Hookflash Transfer

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/itsv21/index.htm

Cisco Mobile Networks—Priority Home Agent Assignment

The mobile router currently preconfigures home agents with different priorities, registering with only the highest priority home agent. However, there are situations in which the mobile router roams to an area where a closer home agent is more desirable to register with. The Cisco Mobile Networks—Priority Home Agent Assignment feature allows a mobile router to register with the closer home agent using the existing home agent priority configurations on the mobile router and care-of address access lists configured on the home agent. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftdynaha.htm

Cisco Mobile Networks—Static Collocated Care-of Address

The Cisco Mobile Networks—Static Collocated Care-of Address feature allows a mobile router to roam to foreign networks where foreign agents are not deployed. Before the introduction of this feature, the mobile router was required to use a foreign agent care-of address when roaming. Now a roaming interface with a static IP address configured on the mobile router itself works as the collocated care-of address (CCoA).

Cisco Mobile Networks—Tunnel Templates for Multicast

The Cisco Mobile Networks—Tunnel Templates for Multicast feature allows the configuration of multicast on statically created tunnels to be applied to dynamic tunnels brought up on the home agent and mobile router. A tunnel template is defined and applied to the tunnels between the home agent and the mobile router. The mobile router can now roam carrying multicast sessions to its mobile networks. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftmultic.htm

Cisco Survivable Remote Site Telephony Version 2.1

The Cisco Survivable Remote Site Telephony (SRST) feature offers enterprises a reliable mechanism for providing continuous IP telephony services to small branch offices in the event of an outage. SRST enables enterprises to build large IP telephony networks using centralized call processing resources.

SRST Version 2.1 provides support for the Cisco IP Phone Extension Module 7914, Unity Voice Mail integration, additional languages for Cisco IP Phone 7940 and Cisco IP Phone 7960 display, higher directory number (DN) maximums, and a new command for creating global prefixes. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/srst21/index.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(11)YT. This release is porting the feature into the Cisco 1750, Cisco 1751, Cisco 2420, Cisco 2610–2613, Cisco 2610XM–2611XM, Cisco 2620–2621, Cisco 2620XM–2621XM, Cisco 2650–2651, Cisco 2650XM–2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, Cisco 3725, Cisco 3745, and Cisco 7200 series platforms.

Class-Based Policer for the DiffServ AF PHB

The Class-Based Policer for the DiffServ AF PHB feature is based on RFC 2697 *A Single Rate Three Color Marker*. The packet stream is metered and packets are marked "conform," "exceed," or "violate." Marking is based on a Committed Information Rate (CIR) and two associated burst sizes, a Committed Burst Size (CBS) and an Excess Burst Size (EBS). A packet is marked "conform" if it does not exceed the CBS, "exceed" if it exceeds the CBS but not the EBS, and "violate" otherwise.

Note This feature was originally introduced in Cisco IOS Release 12.1(5)T. This release is porting the feature into the Cisco 820 platform.

Clear Channel T3/E3 with Integrated CSU/DSU

Nonchannelized (Clear Channel) T3/E3 service is delivered as a T3/E3 pipe with the bandwidth being 28x24x64k for T3 or 16x32x64k for E3. Clear Channel T3/E3 service is generally used in point-to-point applications (one customer sending data to one remote site). Any subdivision of bandwidth is performed at each customer site rather than at the central office. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122yt/122yt11/ft_te3nm.htm

Clear IPC Statistics

This existing feature provides a way to clear and reset the interprocess communications (IPC) statistics. When debugging IPC problems, the ipc stat counters are clearable, making it easier to diagnose the problem.

DHCP Accounting

The DHCP Accounting feature introduces authentication, authorization, and accounting (AAA) and Remote Authentication Dial-In User Service (RADIUS) support for Dynamic Host Configuration Protocol (DHCP) configuration. The introduction of AAA and RADIUS support improves public wireless LAN (PWLAN) security by sending secure START and STOP accounting messages. The configuration of this feature adds a layer of security that allows DHCP lease assignment and termination to be triggered for the appropriate RADIUS START and STOP accounting records so that the session state is properly maintained by upstream devices, such as a Service Selection Gateway (SSG). The additional security provided by this feature can help to prevent unauthorized clients or hackers from gaining illegal entry to the network by spoofing authorized DHCP leases. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftdhcpac.htm

DHCP ODAP Server Support

The DHCP ODAP Server Support feature introduces the capability to configure an IOS Dynamic Host Configuration Protocol (DHCP) server (or router) as a subnet allocation server. This capability allows the IOS DHCP server to be configured with a pool of subnets for lease to On-Demand Address Pool (ODAP) clients. Subnet pools can be configured for global ODAP clients or Multiprotocol Label Switched (MPLS) Virtual Private Network (VPN) ODAP clients on a per-client basis. The DHCP subnet allocation server creates bindings for the subnet leases and stores these leases in the DHCP database. This feature also supports database agents for subnet lease recovery. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftodapss.htm

DHCP Secured IP Address Assignment

The DHCP Secure IP Address Assignment feature introduces the capability to secure ARP table entries to Dynamic Host Configuration Protocol (DHCP) leases in the DHCP database. This feature secures and synchronizes the MAC address of the client to the DHCP binding, preventing unauthorized clients or hackers from spoofing the DHCP server and taking over a DHCP lease of an authorized client. When this feature is enabled and the DHCP server assigns an IP address to the DHCP client, the DHCP server adds a secure ARP entry to the ARP table with the assigned IP address and the MAC address of the client. This ARP entry cannot be updated by any other dynamic ARP packets, and this ARP entry will exist in the ARP table for the configured lease time or as long as the lease is active. The secured ARP entry can be deleted only by an explicit termination message from the DHCP client or by the DHCP server when the DHCP binding expires. This feature can be configured for a new DHCP network or used to upgrade the security of an existing network. The configuration of this feature does not interrupt service and is not visible to the DHCP client. The configuration of this feature does not interrupt service and is not visible to the DHCP client. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftdsiaa.htm

DHCP Server Import All Enhancement

When the import all DHCP pool configuration command is used, the DHCP Server Import All Enhancement feature allows options imported by one subsystem to coexist with options imported from another subsystem. When the session is terminated or the lease is released, the imported options are cleared from the DHCP server database.

DHCP Server—ODAP Support for Non-MPLS VPN Pools

The DHCP Server—On-Demand Address Pool Manager is a feature in which pools of IP addresses can be dynamically increased or reduced in size depending on the address utilization level. On-demand address pools (ODAPs) support address assignment using the Dynamic Host Configuration Protocol (DHCP) for customers using private addresses. Each ODAP is configured and associated with a particular Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN).

The DHCP Server—ODAP Support for Non-MPLS VPN Pools feature enhances the existing feature to provide support for non-MPLS VPN pools. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftondhcp.htm

E1 R2 Signaling

R2 signaling is an international signaling standard that is common to channelized E1 networks. The E1 R2 Signaling feature was introduced in Cisco IOS Release 11.3(2)T and is now supported on Cisco 1751 and Cisco 1760 platforms in Cisco IOS Release 12.2(15)T

EIGRP Nonstop Forwarding (NSF) Awareness

Nonstop Forwarding (NSF) awareness allows a router to assist NSF-capable neighbors to continue forwarding packets during a switchover operation or during a well-known failure condition. The EIGRP Nonstop Forwarding Awareness feature allows an NSF-aware router that is running EIGRP to forward packets along routes that are already known for a router that is performing a switchover operation or is in a well-known failure mode. This capability allows the EIGRP peers of the failing router to retain the routing information that is advertised by the failing router and continue to use this information until the failed router has returned to normal operating behavior and is able to exchange routing information. The peering session is maintained throughout the entire NSF operation.

Enhanced Debug Capabilities for Cisco Voice Gateways

The enhanced debugging capability for Cisco voice gateways provides improvements to the debugging output in order to identify and track a specific call in a multiple-call environment. Before the implementation of this feature, it was difficult to correlate call information between gateways or to identify specific debug messages associated with a single call, when multiple voice calls were simultaneously active. The output was unstructured and presented in a free form.

This feature adds a standardized header to the debug outputs of multiple voice modules, such as voice telephony service provider (VTSP), call control application program interface (CCAPI), session application (SSAPP), and interactive voice response (IVR). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_dbgs2.htm

Enhanced Object Tracking

Prior to the introduction of the Enhanced Object Tracking feature, the Hot Standby Router Protocol (HSRP) had a simple tracking mechanism that allowed you to track the interface line protocol state only. If the line protocol state of the interface went down, the HSRP priority of the router was reduced, allowing another HSRP router with a higher priority to become active. The Enhanced Object Tracking feature separates the tracking mechanism from HSRP and creates a separate standalone tracking process that can be used by any other process as well as by HSRP. This feature allows tracking of other objects in addition to the interface line protocol state.

A client process, such as HSRP, Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP), can now register with the tracking service, its interest in tracking a particular object, such as an interface or a route, and then be notified when the tracked object changes state. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/fthsrptk.htm

Expanded Scope for Cause-Code-Initiated Call Establishment Retries

The Expanded Scope for Cause-Code-Initiated Call Establishment Retries feature enables the gateway to reattempt calls when a disconnect message is received from the public switched telephone network (PSTN) without maintaining extra dial peers. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_ccu.htm

Exporting and Importing RSA Keys

The Exporting and Importing RSA Keys feature allows you to transfer security credentials between devices by exporting and importing RSA keys.

The Exporting and Importing RSA Keys feature allows you to share the private RSA key pair of a router with standby routers, therefore transferring the security credentials between networking devices. The key pair that is shared between two routers will allow one router to immediately and transparently take over the functionality of the other router. If the main router were to fail, the standby router could be dropped into the network to replace the failed router without the need to regenerate keys, reenroll in certification authority (CA), or manually redistribute keys.

You can also use the Exporting and Importing RSA Keys feature to place the same RSA key pair on multiple routers, so that all management stations that use SSH can be configured with a single public RSA key. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_key.htm

Fax and Modem Pass-Through over VoIP

Fax and modem pass-through are now supported on the Cisco 1750 and Cisco 1761 platforms beginning in Cisco IOS Release 12.2(15)T.

Note The Fax and Modem Pass-Through over VoIP feature is also known under the feature title Modem Passthrough over Voice over IP.

On detection of the fax or modem tone on an established VoIP call, the gateways switch into modem fax or pass-through mode: the voice codec and configuration is suspended and the pass-through parameters are loaded for the duration of the fax or modem session. This changes the bandwidth needed for the call to the equivalent of G.711.

With pass-through, the fax or modem traffic is carried between the two gateways in RTP packets, using an uncompressed format resembling the G.711 codec. Packet redundancy may be used to mitigate the effects of packet loss in the IP network. Even so, fax and modem pass-through remain susceptible to packet loss, jitter and latency in the IP network. The two endpoints must be clocked synchronously for this type of transport to work predictably.

The Fax and Modem Pass-Through feature is also known as Voice Band Data (VBD) by the International Telecommunication Union (ITU). VBD refers to the transport of fax or modem signals over a voice channel through a packet network with an encoding appropriate for fax or modem signals. The minimum set of coders for VBD mode is G.711 ulaw and alaw with VAD disabled. For modem transport, Echo cancellation is also be disabled.

Firewall Intrusion Detection System Signature Enhancements

Before the Firewall Intrusion Detection System Signature Enhancements, the Cisco Intrusion Detection System (IDS) contained 59 signatures, which was only a small subset of the signatures supported by Cisco Secure IDS. Firewall Intrusion Detection System (IDS) Signature Enhancements introduces 42 additional IDS signatures to Cisco IOS IDS that are supported by other Cisco products, such as PIX; these newly added signatures are categorized as follows:

- 21 of the 28 most commonly seen signatures in the Security Posture Assessment (SPA) findings
- 6 of the 7 PIX signatures that were unavailable in Cisco IOS IDS

- All 19 of the most dangerous HTTP signatures in the Cisco Secure IDS Network Security Database (NSDB)

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122yu11/ft_fwids.htm

Firewall N2H2 Support

The Cisco IOS Firewall N2H2 Support feature provides users with an additional option when choosing the URL filter vendor. Just like the Websense URL filtering server, N2H2 interacts with your Cisco IOS firewall (also known as Cisco Secure Integrated Software [CSIS]) to allow you to prevent users from accessing specified websites on the basis of some policy. The Cisco IOS firewall works with the N2H2 Internet Filtering Protocol (IFP) server to know whether a particular URL should be allowed or denied (blocked). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122yu11/ft_n2h2.htm

Firewall Support of HTTPS Authentication Proxy

The Firewall Support of HTTPS Authentication Proxy feature allows a user to encrypt the change of the username and password between the HTTP client and the Cisco IOS router via Secure Socket Layer (SSL) when authentication proxy is enabled on the Cisco IOS firewall, thereby ensuring confidentiality of the data that is passing between the HTTP client and the Cisco IOS router. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122yu11/ftfwhttp.htm

Frame Relay Voice-Adaptive Traffic Shaping

The Frame Relay Voice-Adaptive Traffic Shaping feature enables a permanent virtual circuit (PVC) to adjust the rate of traffic on the basis of the presence of packets in the priority queue or H.323 call setup signaling packets. This feature also introduces voice-adaptive fragmentation. Frame Relay voice-adaptive fragmentation allows fragmentation to be turned on when packets are detected in the priority queue or H.323 signaling packets are present and to be turned off when priority queue traffic and signaling packets are not present. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_vats.htm

G.732 Support for the Integrated Signaling Link Terminal

The G.732 Support for the Integrated Signaling Link Terminal feature ports the existing International Telecommunication Union Telecommunication Standardization Sector (ITU-T) G.732 bit error rate (BER) detection and alarm processing functionality from the Cisco Signaling Link Terminal (SLT) onto the Cisco AS5350 and Cisco AS5400 network access server (NAS) platforms. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftg7325x.htm

Gatekeeper Management Statistics

The Gatekeeper Management Statistics feature adds support for gatekeeper performance management parameters that provide statistics that may be used to monitor and troubleshoot a network. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_gms.htm

GLBP: Gateway Load Balancing Protocol

The Gateway Load Balancing Protocol feature provides automatic router backup for IP hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first-hop routers on the LAN combine to offer a single virtual first-hop IP router while sharing the IP packet forwarding load between them. Other routers on the LAN may act as redundant GLBP routers that will become active if any of the existing forwarding routers fail.

This feature was originally introduced in Cisco IOS Release 12.2(14)S. This release is porting the feature into the Cisco 1700 series, Cisco 2600 series, Cisco 3640, and Cisco 3660 platforms. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_glbp.htm

H.323v4 Gateway Zone Prefix Registration Enhancements

The H.323v4 Gateway Zone Prefix Registration Enhancements feature provides support for two capabilities included in H.323 version 4: additive registration and dynamic zone prefix registration. Additive registration allows a gateway to add to or modify a list of aliases contained in a previous registration without first unregistering from the gatekeeper. Dynamic zone prefix registration allows a gateway to register actual public switched telephone network (PSTN) destinations served by the gateway with its gatekeeper. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftgwzpre.htm

HTTP 1.1 Client

This feature implements support for HTTP clients within Cisco IOS software compliant with the HTTP 1.1 standard (RFC 2616). The HTTP 1.1 Client allows the network device to contact a remote web server and obtain content or interact with remote applications. The HTTP 1.1 Client is enabled by default on supported platforms.

HTTP 1.1 Web Server

The HTTP 1.1 Web Server feature provides a consistent interface for users and applications by implementing the HTTP 1.1 standard (RFC 2616). Prior to this release, Cisco software supported only a partial implementation of HTTP 1.0. The integrated HTTP Server API supports server application interfaces. When combined with the HTTPS and HTTP 1.1 Client features, the HTTP 1.1 Web Server feature provides a complete, secure solution for HTTP services to and from Cisco devices. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/fthttp1s.htm

HTTPS–HTTP with SSL 3.0

The HTTPS–HTTP with SSL 3.0 feature provides integrated Secure Socket Layer (SSL) 3.0 support for the HTTP 1.1 Server and Client in Cisco IOS software. SSL provides encryption to allow secure HTTP communications. HTTP with SSL (HTTPS) allows for encrypted HTTP communications with Cisco devices.

IGMP State Limit

The IGMP State Limit feature provides protection against denial of service (DoS) attacks caused by Internet Group Management Protocol (IGMP) packets. The new command-line interface (CLI) introduced by this feature allows you to configure a limit on the number of IGMP states that results from IGMP, IGMP Version 3 lite (IGMP v3lite), and URL Rendezvous Directory (URD) membership reports on a per-interface or global basis. Membership reports in excess of the configured limits will not be entered in the IGMP cache, and traffic for those excess membership reports will not be forwarded. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_igmps.htm

Implementing OSPF for IPv6

The Open Shortest Path First (OSPF) Version 3 for IPv6 (RFC 2740) feature expands on OSPF to provide support for IPv6 routing prefixes. In OSPF for IPv6, the commands used to customize OSPF are in interface configuration mode rather than router configuration mode. When using a nonbroadcast multiaccess (NBMA) interface in OSPF for IPv6, users must manually configure the router in order to detect neighbors.

Integrated IS-IS Multi-Topology Support for IPv6

The Integrated IS-IS Multi-Topology Support for IPv6 feature provides support for routing IPv6 prefixes in Intermediate System-to-Intermediate System (IS-IS) using a multi-topology solution.

Integrated IS-IS Nonstop Forwarding (NSF) Awareness

The Integrated IS-IS Nonstop Forwarding (NSF) Awareness feature allows customer premises equipment (CPE) routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/isnsfawa.ht

Integrated Voice and Data WAN on T1/E1 Interfaces Using the AIM-ATM-VOICE-30 Module

The Integrated Voice and Data WAN on T1/E1 Interfaces Using the AIM-ATM-VOICE-30 Module feature provides configuration enhancements for the AIM-ATM-VOICE-30 digital signaling processor (DSP) card on the Cisco 2600 series, Cisco 2600XM, Cisco 3660, Cisco 3725, and Cisco 3745. This feature provides a migration path to higher bandwidth without the need to change transport facilities and provides a voice processing (termination) solution with AIM-ATM-VOICE-30 without consuming a network module slot. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbckaim.htm

IP Access List Entry Sequence Numbering

Users can apply sequence numbers to permit or deny statements and also reorder, add, or remove such statements from a named IP access list. This feature makes revising IP access lists much easier. Prior to this feature, users could add access list entries to the end of an access list only; therefore needing to add statements anywhere except the end required reconfiguring the entire access list.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsaclseq.htm

IPMROUTE-STD-MIB

This feature introduces support for the IPMROUTE-STD-MIB in Cisco IOS software. IPMROUTE-STD-MIB, as defined in RFC 2932, is a module for management of IP multicast routing in a manner independent of the specific multicast routing protocol in use. Support for this MIB replaces the draft form of the IPMROUTE-MIB.

The IPMROUTE-STD-MIB supports all the MIB objects of the IPMROUTE-MIB and in addition supports the following four new MIB objects:

1. ipMRouteEntryCount
2. ipMRouteHCOctets
3. ipMRouteInterfaceHCInMcastOctets
4. ipMRouteInterfaceHCOutMcastOctets

Note The ipMRouteScopeNameTable MIB object is not supported because it is not relevant to multicast routers.

IPSec VPN Accounting

The IPSec VPN Accounting feature allows for a session to be accounted for by indicating when the session starts and when it stops. Additionally, session identifying information and session usage information will be passed to the RADIUS server via RADIUS attributes and vendor-specific attributes (VSAs). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_evpna.htm

IPv6 ISATAP Tunnel Support

The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is an automatic overlay tunneling mechanism that uses the underlying IPv4 network as a nonbroadcast multiaccess (NBMA) link layer for IPv6. The IPv4 address is encoded in the last 32 bits of the IPv6 address, enabling automatic IPv6-in-IPv4 tunneling within an IPv4 network. ISATAP tunnels allow individual IPv4/IPv6 dual-stack hosts within a site to connect to an IPv6 network using the IPv4 infrastructure. ISATAP uses a normal global IPv6 prefix (/64), that can be used with both local and global unicast IPv6 prefixes, enabling IPv6 routing on the Internet. For additional information, refer to the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6/ipv6imp/sa_tunv6.htm

IPv6 MIB Support

IPv6 MIBs are now available for managing IPv6 traffic. Supported MIBs include the CISCO-IETF-IP-MIB and CISCO-IETF-IP-FORWARDING-MIB.

IPv6 Provider Edge Router over MPLS

The IPv6 Provider Edge Router over MPLS (Cisco 6PE) feature allows service providers that are running an MPLS/IPv4 infrastructure to offer IPv6 services on an Multiprotocol Label Switching (MPLS) network. A Cisco 6PE-enabled backbone allows IPv6 domains to communicate with each other over an MPLS IPv4 core network. A Cisco 6PE implementation requires no backbone infrastructure upgrades and no reconfiguration of core routers, because forwarding is based on labels rather than on the IP header itself.

Additionally, the inherent Virtual Private Network (VPN) and Traffic Engineering (TE) services available within an MPLS environment allow IPv6 networks to be combined into VPNs or extranets over an infrastructure that supports IPv4 VPNs and MPLS-TE.

The provider edge (PE) routers at each end of the MPLS network must be IPv6-enabled. The PE routers apply an appropriate label for the address in the packet to reach the other side of the MPLS backbone. This is similar to tunneling because it allows IPv6 traffic to be transported over MPLS without the routers in the backbone being aware of the IPv6 traffic. An MPLS packet enters and exits the MPLS network on different routers, and each router must be IPv6- and 6PE-enabled.

For more information about the IPv6 Provider Edge Router over MPLS (Cisco 6PE) feature, refer to the following document:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/iosip_an.htm

ISDN Generic Transparency Descriptor (GTD) for Setup Message

The ISDN Generic Transparency Descriptor for Setup Message feature provides support for mapping ISDN information elements (IEs) to corresponding GTD parameters. Supported IEs and GTD parameters include the following:

- Originating Line Information (OLI)
- Bearer Capability (USI and TMR)
- Called Party Number (CPN)
- Calling Party Number (CGN)
- Redirecting Number (RGN, OCN, and RNI)

This feature allows networks to do the following:

- Extract Originating Line Information (OLI) to identify pay telephone calls and pass on applicable charges.
- Generate billing records that can be used to validate pay telephone operator settlement requests.

Cisco implements this feature on Cisco IOS gateways by providing a mechanism to allow creating and passing the Q931 Setup message and its parameters in a GTD format. The Setup message, sent by the gateway to initiate call establishment, is mapped to the GTD Initial Address Message (IAM). Generic transparency descriptors represent parameters within signaling messages and enable transport of signaling data in a standard format across network components and applications. The GTD mechanism allows them to share signaling data and achieve interworking between different signaling types.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftgtdisd.htm

ISDN PRI-SLT

The ISDN PRI-SLT feature allows you to release the ISDN PRI signaling time slot for Redundant Link Manager (RLM) configurations and for Signaling System 7 (SS7) applications in integrated Signaling Link Terminal (SLT) configurations. This feature supports the use of DS0 time slots for SS7 links and allows the coexistence of SS7 links and PRI voice and data bearer channels on the same T1 or E1 controller span. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_8/ftprislt.htm

ISDN Progress Indicator Support for SIP Using 183 Session Progress

The ISDN Progress Indicator Support for SIP Using 183 Session Progress feature adds the SIP 183 Session Progress and Ringing messages to better map to the ISDN/CAS messages.

The ISDN Progress Indicator Support for SIP Using 183 Session Progress feature was previously released in Cisco IOS Release 12.1(5)T. This feature has been added on the Cisco 1751 and the Cisco 1760 in Cisco IOS Release 12.2(15)T.

L2TP Dial-Out Load Balancing and Redundancy

The L2TP Dial-Out Load Balancing and Redundancy feature enables an L2TP network server (LNS) to dial out to multiple L2TP access concentrators (LACs). When the LAC with the highest priority goes down, it is possible for the LNS to failover to another lower priority LAC. The LNS can also load-balance the sessions between multiple LACs that have the same priority settings. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftl2tlbr.htm

L2TP Large-Scale Dial-Out per-User Attribute via AAA

The L2TP Large-Scale Dial-Out per-User Attribute via AAA feature enhances Layer 2 Tunneling Protocol (L2TP) to support per-user attributes using authentication, authorization, and accounting (AAA) for large-scale dial-out. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftl2taaa.htm

Malicious Caller Identification (MCID) Invocation Support for Enterprise Networks

The Malicious Caller Identification (MCID) Invocation Support for Enterprise Networks feature enables a called party inside an enterprise network to use a configurable sequence of digits to notify the local law enforcement agency of a malicious call. MCID uses Tool Command Language (TCL) and interactive voice response (IVR) to trigger the gateway to send calling number information to the authorities.

The feature is platform independent; uses dual tone multifrequency (DTMF) tones to generate the trigger; and operates in both H.323 and Session Initiation Protocol (SIP) voice gateways and on all phones. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftmcid.htm

Measurement-Based Call Admission Control for SIP

The Measurement-Based Call Admission Control for SIP feature implements support within Session Initiation Protocol (SIP) to monitor IP network capacity and check the availability of router and interface resources, and to decide if adequate resources are available to carry a successful Voice over IP (VoIP) session. This feature also implements a mechanism to prevent calls that arrive from the IP network from entering the gateway when required resources are not available to process the call. This feature also provides the ability to support measurement-based call admission control processes as well as check for resource availability. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftcacsip.htm

MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles

The MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles feature implements the following Media Gateway Control Protocol (MGCP) protocols on the supported Cisco media gateways:

- MGCP 1.0 (RFC 2705)
- Network-based Call Signaling (NCS) 1.0, the PacketCable profile of MGCP 1.0 for residential gateways (RGWs)
- Trunking Gateway Control Protocol (TGCP) 1.0, the PacketCable profile of MGCP 1.0 for trunking gateways (TGWs)

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_24mgl.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco 1751 and Cisco 1760 platforms.

MGCP Based Fax (T.38) and DTMF Relay

This feature adds support for T.38 fax relay and dual tone multifrequency (DTMF) relay with Media Gateway Control Protocols (MGCP). This feature provides two modes of implementation for each component: gateway (GW)-controlled mode and call agent (CA)-controlled mode. In GW-controlled mode, GWs negotiate DTMF and fax relay transmission by exchanging capability information in Session Description Protocol (SDP) messages. That transmission is transparent to the CA. GW-controlled mode allows use of the MGCP-Based Fax (T.38) and DTMF (IETF RFC 2833) Relay feature without upgrading the CA software to support the feature. In CA-controlled mode, CAs use MGCP messagir to instruct GWs to process fax and DTMF traffic. For MGCP T.38 Fax Relay, the CAs can also instruct GWs to revert to GW-controlled mode if the CA is unable to handle the fax control messaging traffic; for example, in overloaded or congested networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmgcpfx.htm

The MGC Protocol Based Fax (T.38) and DTMF (IETF RFC 2833) Relay feature was previously released in Cisco IOS Release 12.2(8)T on the Cisco 3600 series and Cisco MC3810, and in Cisco IOS Release 12.2(11)T on the Cisco AS5300, Cisco AS5400, and Cisco AS5850. This feature has been added on the Cisco 1751 and the Cisco 1760 in Cisco IOS Release 12.2(15)T.

MGCP Basic CLASS and Operator Services

The Media Gateway Control Protocol (MGCP) Basic CLASS and Operator Services feature provides CLASS and 3-way calling functionality using the Simple Gateway Control Protocol (SGCP) and MGCP protocols.

MGCP VoIP Call Admission Control

The MGCP VoIP Call Admission Control (CAC) feature determines if calls can be accepted on the IP network on the basis of available network resources. Before this release, Media Gateway Control Protocol (MGCP) Voice over IP (VoIP) calls were established regardless of the available resources on the gateway or network. The gateway had no mechanism for gracefully refusing calls if resources were not available to process the call. New calls would fail with unexpected behavior and in-progress calls would experience quality-related problems.

The MGCP VoIP Call Admission Control feature provides three CAC mechanisms to address the need for improved quality and predictable gateway behavior. The first mechanism is local/system CAC, which provides the ability to gracefully refuse calls on the basis of the availability of local gateway call processing resources such as CPU utilization and memory. The second CAC mechanism provides synchronization with Resource Reservation Protocol (RSVP) and reports the reservation request to the call agent. The third mechanism provides network congestion detection to gracefully refuse calls on the basis of a measured level of congestion.

The MGCP VoIP Call Admission Control feature was previously released in Cisco IOS Release 12.2(8)T and is now supported on the Cisco 1751 and Cisco 1760 platforms.

Mobile IP—Home Agent Accounting

In Cisco IOS Mobile IP, the home agent keeps track of the location of the mobile node as it roams away from its home network and forwards all traffic destined to the mobile node to its new location on the Internet. The Mobile IP—Home Agent Accounting feature allows the home agent to generate the following three new accounting messages that are forwarded to the Service Selection Gateway (SSG):

- Accounting Start
- Accounting Update
- Accounting Stop

The SSG acts as the proxy server for the authentication, authorization, and accounting (AAA) server and acknowledges the accounting messages sent by the home agent. The accounting records generated by the home agent can be stored on the AAA server and used by Internet service providers (ISPs) for billing, capacity planning, and operations. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/fthaacct.htm

MPLS VPN—MIB Support

The MPLS VPN—MIB Support feature provides Simple Network Management Protocol (SNMP) agent support in Cisco IOS software for Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) management, as implemented in the draft *MPLS/BGP Virtual Private Network Management Information Base Using SMIv2* (*draft-ietf-ppvpn-mpls-vpn-mib-03.txt*). The Provider-Provisioned VPN (PPVPN)-MPLS-VPN MIB provides access to VPN routing/forwarding instance (VRF) information, interfaces included in the VRF, and other configuration and monitoring information.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftvnmb15.htm

The MPLS VPN—MIB Support feature was introduced in Cisco IOS Release 12.0(21)ST. The PPVPN-MPLS-VPN MIB notifications were supported in Cisco IOS Release 12.2(13)T. The PPVPN-MPLS-VPN MIB tables were integrated into Cisco IOS Release 12.2(15)T.

MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE)

The MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE) feature provides the Enhanced Interior Gateway Routing Protocol (EIGRP) with the capability to redistribute routes through a Border Gateway Protocol (BGP) Virtual Private Network (VPN) cloud. This feature is configured only on PE routers, requiring no upgrade or configuration changes to customer equipment. This feature also introduces EIGRP support for Multiprotocol Label Switching (MPLS) and BGP extended community attributes. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/fteipece.htm

Multicast Subsecond Convergence

The Multicast Subsecond Convergence feature comprises a comprehensive set of features and protocol enhancements that provide for improved scalability and convergence in multicast-based services. This feature set provides for the ability to scale to larger service levels and to recover multicast forwarding after service failure in subsecond time frames.

Multicast subsecond convergence allows you to send Protocol Independent Multicast (PIM) router-query messages (PIM hellos) every few milliseconds. In earlier releases, you could send the PIM hellos every few seconds. By enabling a router to send PIM hello messages more often, this feature allows the router to discover unresponsive neighbors more quickly. As a result, the router can implement failover or recovery procedures more efficiently.

The scalability enhancements improve on the efficiency of handling increases (or decreases) in service users (receivers) and service load (sources or content). Scalability enhancements in this release include the following:

- Improved Internet Group Management Protocol (IGMP) and PIM state maintenance through new timer management techniques
- Improved scaling of the Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache

The scalability enhancements provide the following benefits:

- Increased potential PIM multicast route (mroute), IGMP, and MSDP SA cache state capacity
- Decreased CPU usage

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fs_subcv.htm

Multiple OPC Support for the Cisco Signaling Link Terminal

Multiple OPC Support for the Cisco Signaling Link Terminal (SLT) feature allows Cisco SLTs to access multiple Signaling System 7 (SS7) point codes (PCs) on a media gateway controller (MGC).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftsltopc.htm

NAT Support for IPSec ESP—Phase II

The NAT Support for IPSec ESP—Phase II feature allows multiple concurrent IP Security (IPSec) Encapsulating Security Payload (ESP) tunnels or connections through a Cisco IOS Network Address Translation (NAT) device configured in overload or Port Address Translation (PAT) mode. The IPSec ESP deployment does not need to use wrapper techniques that typically use the User Datagram Protocol (UDP) to pass through the NAT router. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftsecnat.htm

Network-Based Application Recognition Protocol Discovery Management Information Base

The existing Network-Based Application Recognition (NBAR) feature is used to identify protocols so that traffic can be classified appropriately for quality of service purposes. NBAR also contains a protocol discovery feature that displays for the user any NBAR-supported protocol traffic that is traversing an interface.

The NBAR Protocol Discovery MIB expands the capabilities of NBAR protocol discovery by providing the following new protocol discovery functionality through simple network management protocol (SNMP):

- Enables or disables protocol discovery per interface.
- Displays protocol discovery statistics.
- Configures and displays multiple top-n tables that list protocols by bandwidth usage.

Configure thresholds based on traffic of particular NBAR-supported protocols or applications that report breaches and send notifications when these thresholds are crossed. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftpdmib.htm

No Service Password-Recovery

The No Service Password-Recovery feature disables password-recovery capability for better console security.

OSPF Forwarding Address Suppression in Translated Type-5 LSAs

The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes a not-so-stubby area (NSSA) area border router (ABR) to translate Type-7 link state advertisements (LSAs) to Type-5 LSAs, but use the address 0.0.0.0 for the forwarding address instead of that specified in the Type-7 LSA. This feature causes routers that are configured not to advertise forwarding addresses into the backbone to direct forwarded traffic to the translating NSSA ABRs. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftoadsup.htm

OSPF Inbound Filtering Using Route Maps with a Distribute List

Users can define a route map to prevent Open Shortest Path First (OSPF) routes from being added to the routing table. In the route map, the user can match on any attribute of the OSPF route.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/routmap.htm

OSPF Nonstop Forwarding (NSF) Awareness

The OSPF Nonstop Forwarding (NSF) Awareness feature allows customer premises equipment (CPE) routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftosnsfa.htm

OSPF Shortest Path First Throttling

The OSPF Shortest Path First Throttling feature makes it possible to configure Shortest Path First (SPF) scheduling in millisecond intervals and to potentially delay SPF calculations during network instability. SPF is scheduled to calculate the Shortest Path Tree (SPT) when there is a change in topology. One SPF run may include multiple topology change events.

The interval at which the SPF calculations occur is chosen dynamically and is based on the frequency of topology changes in the network. The chosen interval is within the boundary of the user-specified value ranges. If network topology is unstable, SPF throttling calculates SPF scheduling intervals to be longer until the topology becomes stable. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsspftrl.htm

OSPF Support for Fast Hello Packets

The OSPF Support for Fast Hello Packets feature provides a way to configure the sending of hello packets in intervals less than 1 second. Such a configuration would result in faster convergence in an Open Shortest Path First (OSPF) network. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/fasthelo.htm

Per-User QoS via AAA Policy Name

The Per-User QoS via AAA Policy Name feature provides the ability to download a policy name that describes quality of service (QoS) parameters for a user session from a RADIUS server and apply them for the particular session. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_puq.htm

Per VRF AAA

The Per VRF AAA feature allows authentication, authorization, and accounting (AAA) on the basis of Virtual Private Network (VPN) routing and forwarding (VRF) instances. For Cisco IOS Release 12.2(15)T or later releases, you can use a customer template which may be stored either locally or remotely, and AAA services can be performed on the information that is stored in the customer template. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvrfaaa.htm

PPPoE Connection Throttling

This feature will throttle the PPP over Ethernet (PPPoE) connection requests to prevent any denial of service attacks. It will implement per-mac/per-vc initiated session rate throttling in the PPPoE server to limit the session initiate count during a specific period of time.

PPPoE Profiles

The PPPoE Profiles feature introduces PPP over Ethernet (PPPoE) profiles, which contain configuration information for a group of PPPoE sessions. Multiple PPPoE profiles can be defined on a device, allowing different virtual templates and other PPPoE configuration parameters to be assigned to different Ethernet interfaces, VLANs, and ATM permanent virtual circuits (PVCs). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftpprfls.htm

PRI QSIG Protocol

QSIG is a standardized PBX signaling protocol used primarily in Europe over E1 and BRI trunks and occasionally in North America over T1 trunks. The PRI QSIG Protocol feature provides QSIG signalling over PRI trunks

RADIUS Support of 56-Bit Acct Session-Id

The Radius Support of 56-Bit Acct Session-Id feature introduces a new 32-bit authentication, authorization, and accounting (AAA) variable, acct-session-id-count. The first 8 bits of the acct-session-id-count variable are reserved for the unique-ident, a unique number assigned to the accounting session that is preserved between reloads. The acct-session-id-count variable is used in addition to the existing 32-bit acct-session-id variable, RADIUS Attribute 44. This provides 56 bits to represent the actual accounting session ID. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftradaid.htm

RADIUS Timeout Set During Pre-Authentication

The RADIUS Timeout Set During Pre-Authentication feature provides RADIUS timeout values during the pre-authentication phase of a session, and the values are not overwritten in later phases of the same session. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftattr27.htm

RSVP Message Authentication

The Resource Reservation Protocol (RSVP) Message Authentication feature permits neighbors in an RSVP network to use a secure hash to sign all RSVP signaling messages digitally, thus allowing the receiver of an RSVP message to verify the sender of the message without relying solely on the sender's IP address, as is done by issuing the **ip rsvp neighbor** command with an access control list (ACL). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftrsvpma.htm

RSVP Support for RTP Header Compression, Phase 1

The Resource Reservation Protocol (RSVP) Support for Real-Time Transport Protocol (RTP) Header Compression, Phase 1 feature provides a method for decreasing a flow's reserved bandwidth requirements so that a physical link can accommodate more voice calls. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftrsvpcf.htm

SIP Call Transfer and Call Forwarding Supplementary Services

The SIP Call Transfer and Call Forwarding Supplementary Services feature introduces the ability of Session Initiation Protocol (SIP) gateways to initiate blind or attended call transfers. Release Link Trunking (RLT) functionality was also added with this feature. With RLT, SIP blind call transfers can now be triggered by channel-associated signaling (CAS) trunk signaling. Finally, the SIP Call Transfer and Call Forwarding Supplementary Services feature implements SIP support of call forwarding requests from a Cisco IOS gateway.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftsipcal.htm

SIP—Configurable PSTN Cause Code Mapping

For calls to be established between a session initiation protocol (SIP) network and a PSTN network, the two networks must be able to interoperate. One aspect of their interoperation is the mapping of PSTN cause codes, which indicate reasons for Public Switched Telephone Network (PSTN) call failure or completion, for SIP status codes or events. The opposite is also true: SIP status codes or events are mapped to PSTN cause codes. Event mapping tables found in this document show the standard or default mappings between SIP and PSTN.

However, you may want to customize the SIP user agent software to override the default mappings between the SIP and PSTN networks. The Configurable PSTN Cause Code to SIP Response Mapping feature allows you to configure specific map settings between the PSTN and SIP networks. Thus, any SIP status code can be mapped to any PSTN cause code, or vice versa. When set, these settings can be stored in the NVRAM and are restored automatically on bootup.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmap.htm

Note This feature was previously released in Cisco IOS Release 12.2(8)T for the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers as Configurable PSTN Cause Code to SIP Response Mapping. This release is porting the feature into the Cisco 1751 and Cisco 1760 platforms.

SIP Diversion Header Implementation for Redirecting Number

SIP is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to the ITU-T H.323 specification. SIP is defined by RFC 2543 and is used for multimedia call session setup and control over IP networks. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/sipcf2.htm

Note This feature was originally introduced in Cisco IOS Release 12.1(3)T. This release ports the feature into the Cisco 1751 and Cisco 1760 platforms.

SIP—DNS SRV RFC2782 Compliance

Session Initiation Protocol (SIP) on Cisco Voice over IP (VoIP) gateways uses Domain Name System Server (DNS SRV) query to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." and is attached to the fully qualified domain name (FQDN) of the next hop SIP server. This prefix style, from RFC 2052, has always been available; however, with this release, a second style is also available. The second style complies with RFC 2782 and prepends the protocol label with an underscore "_"; as in "_protocol._transport." The addition of the underscore reduces the risk of the same name being used for unrelated purposes. The form compliant with RFC 2782 is the default style. Use the **srv version** command to configure the DNS SRV feature.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/vvfresrv.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco 1751 and Cisco 1760 platforms.

SIP Gateway Support for Third Party Call Control

SIP is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to the ITU-T H.323 specification. SIP is defined by RFC 2543 and is used for multimedia call session setup and control over IP networks. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/sipcf2.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release ports the feature into the Cisco 1751 and Cisco 1760 platforms.

SIP Gateway Support of RSVP and TEL URL

The SIP Gateway Support of RSVP and TEL URL feature also supports Telephone Uniform Resource Locators or TEL URLs. Currently Session Initiation Protocol (SIP) gateways support URLs in the SIP format. SIP URLs are used in SIP messages to indicate the originator, recipient, and destination of the SIP request. However, SIP gateways may also encounter URLs in other formats, such as TEL URLs. TEL URLs describe voice call connections. They also enable the gateway to accept TEL calls sent through the Internet and to generate TEL URLs in the request line of outgoing INVITE requests.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/vvfresrv.htm

Note This feature was previously released in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco 1751 and Cisco 1760 platforms.

SIP Intra-gateway Hairpinning

SIP hairpinning is a call routing capability in which an incoming call on a specific gateway is signaled through the IP network and back out the same gateway. This call can be a public switched telephone network (PSTN) call routed into the IP network and back out to the PSTN over the same gateway.

Similarly, SIP hairpinning can be a call signaled from a line (for example, a telephone line) to the IP network and back out to a line on the same access gateway. With SIP hairpinning, unique gateways for ingress and egress are no longer necessary.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco 1751 and Cisco 1760 platforms.

SIP INVITE Request with Malformed Via Header

SIP INVITE requests that a user or service participate in a session. Each INVITE contains a Via header that indicates the transport path taken by the request so far and where to send a response. In the past, when an INVITE contained a malformed Via header, the gateway would print a debug message and discard the INVITE without incrementing a counter. However, the printed debug message was often inadequate, and it was difficult to detect that messages were being discarded.

The SIP INVITE Request with Malformed Via Header feature provides a response to the malformed request. A counter, Client Error: Bad Request, increments when a response is sent for a malformed Via field. Bad Request is a class 400 response and includes the explanation Malformed Via Field. The response is sent to the source IP address (the IP address where the SIP request originated) at User Datagram Protocol (UDP) port 5060.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmalvia.htm

Note This feature was previously released in Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers. This release ports the feature into the Cisco 1751 and Cisco 1760 platforms.

SIP: ISDN Suspend/Resume Support

The SIP: ISDN Suspend/Resume Support feature adds Session Initiation Protocol (SIP) call-hold support to SIP gateways when an ISDN Suspend event is triggered. Because Suspend and Resume support already exists for H.323, the SIP implementation of Suspend and Resume provides feature parity. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftsusres.htm

SIP—Session Initiation Protocol for VoIP Enhancements

Voice over IP (VoIP) currently implements the International Telecommunication Union (ITU)'s H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. The Session Initiation Protocol (SIP) is a new protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP. SIP features are compliant with IETF RFC 2543, *SIP: Session Initiation Protocol*, published in March 1999.

The Cisco SIP functionality, introduced in Cisco IOS Release 12.1(1)T and enhanced in Cisco IOS Release 12.1(3)T, enables Cisco access platforms to signal the setup of voice and multimedia calls over IP networks. This release ports the feature into the Cisco 1751 and Cisco 1760 platforms. The SIP feature also provides nonproprietary advantages in the areas of

- Protocol extensibility
- System scalability
- Personal mobility services
- Interoperability with different vendors

SIP Support for Media Forking

The SIP Support for Media Forking feature provides the ability for Session Initiation Protocol (SIP) networks to create midcall multiple streams (or branches) of audio. The multiple streams of audio are associated with a single call, but can be sent to several different destinations. The SIP Support for Media Forking feature allows service providers to use technologies such as speech recognition, voice authentication, and text-to-speech conversion to provide sophisticated services to their end-user customers. An example is a web-browsing application that uses voice recognition and text-to-speech (TTS) technology to make reservations, verify shipments, or order products. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftspfork.htm

SIP T.38 Fax Relay

The SIP T.38 Fax Relay feature adds standards-based fax support to session initiation protocol (SIP) and conforms to ITU-T T.38 Procedures for real-time Group 3 facsimile communication over IP networks. The ITU-T standard specifies real-time transmission of faxes between two regular fax terminals over an IP network. Much like a voice call, SIP T.38 Fax Relay requires call establishment, data transmission, and release signaling.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftsipfax.htm

Note This feature was previously released in Cisco IOS Release 12.2(8)T for the Cisco 2600 series and Cisco 3600 series routers. This release ports the feature into the Cisco 1751 and Cisco 1760 platforms.

SIP User Agent MIB

The Session Initiation Protocol (SIP) User Agent Client (UAC) and User Agent Server (UAS) are manageable by an SNMP-based network management platform, such as the Cisco Voice Manager. This release ports the feature to the Cisco 1750 and Cisco 1761 platforms. The SIP MIB has been defined, will be submitted to the IETF, and will be implemented on those platforms.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB web site on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Source Interface Selection for Outgoing Traffic with Certificate Authority

The Source Interface Selection for Outgoing Traffic with Certificate Authority feature allows you to specify the address of an interface to be used as the source address for all outgoing TCP connections when a designated trustpoint has been configured. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_asish.htm

Support for Bridged RFC 1483 Encapsulated Traffic over ATM SVCs

The Support for Bridged RFC 1483 Encapsulated Traffic over ATM SVCs feature allows you to send bridged RFC 1483 encapsulated packets over ATM switched virtual circuits (SVCs). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftbridge.htm

Support for IUA with SCTP for Cisco Access Servers

The Support for IUA with SCTP for Cisco Access Servers feature supports the IDSN User Adaptation (IUA) Layer with Stream Control Transmission Protocol (SCTP) for the Cisco AS5x00 network access servers (NASs) and the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series. This feature is to be used as an alternative to the existing IP-based User Datagram Protocol-to-Reliable Link Manager (UDP-to-RLM) transport between the Cisco PGW2200 and Cisco gateways. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftgkrup.htm

T1 Channel Associated Signaling (CAS)

Channel Associated Signaling (CAS) is the transmission of signaling information within the voice channel. Support for CAS is now available on T1 interfaces.

T.37 for Cisco 7200

This feature adds T.37 standards-based store-and-forward fax protocol support for H.323 gateways and gatekeepers to the Cisco 7200 series. T.37 is an ITU-T recommended standard for store-and-forward fax that enables Cisco gateways and gatekeepers to interwork with other Cisco gateways and third-party H.323 devices that support the T.37 protocol.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/index.htm

T.37 store-and-forward fax was originally supported in Cisco IOS Rélease 12.1(5)T on the Cisco AS5300 platform. In Cisco IOS Release 12.2(8)T, support was added on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745. In Cisco IOS Release 12.2(13)T, support was added on the Cisco AS5350 and the Cisco AS5400. Cisco IOS Release 12.2(15)T adds support on the Cisco 7200 series.

Tokenless Call Authorization

The Tokenless Call Authorization feature provides a statically configured access list of authorized H.323 endpoints for the Cisco IOS gatekeeper. The gatekeeper accepts calls from endpoints on the list. This security feature is an alternative to Interzone ClearTokens (IZCTs) and Cisco Access Tokens (CATs), and can be used with Cisco CallManager. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_tklss.htm

Tunneled GR-303 for the Cisco Cable Modem

The Tunneled GR-303 Support feature enables the Cisco uBR925 cable access router to send and receive call control messages using GR-303 signaling, in addition to the Media Gateway Control Protocol (MGCP) signaling that was previously supported. This allows the Cisco uBR925 router to support advanced call features such as caller ID and call waiting, using both GR-303 and MGCP signaling. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/dtgrmgcp.htm

UDP Forwarding Support of IP Redundancy Virtual Router Group (VRG)

User Datagram Protocol (UDP) forwarding is used in Cisco IOS software to forward broadcast and multicast packets received for a specific IP address. Virtual Router Group (VRG) support is currently implemented with the Hot Standby Routing Protocol (HSRP), and it allows a set of routers to be grouped as a logical router that answers to a well known IP address. The UDP Forwarding Support of IP Redundancy Virtual Router Group (VRG) feature enables UDP forwarding to be VRG aware, resulting in forwarding only to the active router in the VRG. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftudpvrg.htm

V.92 and V.44 Support for Digital Modems

The V.92 and V.44 Support for Digital Modems feature supports the V.92 Modem on Hold and V.92 Quick Connect portions of the new V.92 modem standard, and the new V.44 LZJH compression standard based on Lempel-Ziv, on the Cisco 3600 and Cisco 3700 series router platforms. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122yt/122yt11/ftv92_44.htm

VRF-Aware IPSec

The VRF-Aware IPSec feature introduces IP Security (IPSec) tunnel mapping to Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). Using the VRF-Aware IPSec feature, you can map IPSec tunnels to virtual routing and forwarding (VRF) instances using single public-facing addresses.

A VRF instance is a per-VPN routing information repository that defines the VPN membership of a customer site attached to the provider edge (PE) router. A VRF comprises an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table. A separate set of routing and CEF tables is maintained for each VPN customer.

The MPLS distribution protocol is a high-performance packet-forwarding technology that integrates the performance and traffic management capabilities of data link layer switching with the scalability, flexibility, and performance of network-layer routing. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_vrfip.htm

XML Interface to Syslog Messages

The Cisco IOS system logging (Syslog) process allows the system to report and save important error messages, either locally or to a remote logging server. These Syslog messages include system error messages and debugging output sent during network operation to assist users and Cisco TAC engineers with identifying the type and severity of a problem. Syslog messages can be sent to the console, a monitor (TTY), a buffer, or a remote host.

The XML Interface to Syslog Messages features provides Command Line Interface (CLI) commands for enabling syslog messages to be sent in an XML format. XML (Extensible Markup Language), a derivative of SGML, provides a representation scheme to structuralize consistently formatted data such as that found in Syslog messages. This feature defines a closed set of meaningful XML tags for Syslog messages. Logs in a standardized XML format can be more readily used in external customized monitoring tools. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftxmlsys.htm

New Hardware Features Supported in Cisco IOS Release 12.2(13)T

The following new hardware features are supported in Cisco IOS Release 12.2(13)T. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

Catalyst 4224 Access Gateway Switch

The Cisco Catalyst 4224 Access Gateway Switch (Catalyst 4224) is an integrated switch/router that provides Voice over IP (VoIP) gateway and IP telephony services to a small branch office. The Cisco Catalyst 4224 provides an integrated switch and WAN/voice gateway for enterprise satellite offices with up to 24 users. It is intended to work in conjunction with a Cisco Call Manager cluster from the central site with fail over capabilities to allow local calls and basic PBX features.

For information about Cisco Catalyst 4224 configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4224/index.htm

Cisco 3631 Router Enhanced Functionality

In Cisco IOS Release 12.2(13)T, the Cisco 3631 will support additional functionality. Beginning in this release, this router will support the following interfaces:

- NM-T3
- NM-E3
- NM-1FE2W
- NM-2FE2W
- NM-2W
- NM-8B-S/T
- NM-8B-U
- NM-1CEB
- NM-1CEU
- NM-2CEB
- NM-2CEU
- ETM

For more information about network module configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/index.htm

For more information about WAN interface card (WIC) configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/wic_inst/wic_doc/index.htm

Cisco 3725 Router, Cisco 3745 Router, Cisco 2691 Router Enhanced Functionality

In Cisco IOS Release 12.2(13)T, the Cisco 3725, Cisco 3745, and Cisco 2691 routers will support additional functionality. Beginning in this release, these routers will support the following interfaces:

- AIM-ATM
- AIM-VOICE-30
- AIM-ATM-VOICE-30
- AIM-VPNII
- OC-3 NMs (multimode, single-mode intermediate reach and single-mode long reach)

- WIC-1SHDSL
- VIC-2BRI-NT/TE

For more information about network module configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/nm_inst/nm-doc/index.htm

For more information about WAN interface card (WIC) configuration, see the following:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/hw_inst/wic_inst/wic_doc/index.htm

Cisco 7401 ASR-BB and Cisco 7401 ASR-CP

The Cisco 7401 ASR-BB and Cisco 7401 ASR-CP are now supported on Cisco IOS Release 12.2 T.

Content Engine Network Module for Caching and Content Delivery

The Content Engine (CE) Network Module for Caching and Content Delivery offers the ability to integrate the features of Cisco Application and Content Networking System (ACNS) software into branch office platforms. The CE network module combines the Content Caching, Content Filtering and Content Delivery features of ACNS with robust branch office routing and is supported on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

The CE network module can operate as a stand-alone cache or in an integrated enterprise content delivery network (E-CDN) environment. As one element of an E-CDN, the CE network module can be deployed with a combination of other content engines, content routers, content services switches, and content distribution managers to create a complete content delivery network system.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_1cenm.htm

PA-MC-8TE1+

The Cisco PA-MC-8TE1+ is a single-wide port adapter designed to provide a full eight-port PRI multichannel solution for the Cisco 7200 and Cisco 7400. The interfaces can be channelized, fractional or ISDN-PRI, or unframed (E1) with up to 256 independent HDLC channels definable for T1 and E1 applications.

SRP MIB for DPT-OC12 WAN Card

This feature provides the SRP MIB for PA-SRP-OC12xx and SRPIP-OC12xx cards for the Cisco 7200 and Cisco 7500 series routers.

Unchannelized support for PA-MC-2T3+ port adapter

The PA-MC-2T3+ is a single-width port adapter that provides two T3 interface connections. Each T3 interface can now be independently configured to be either channelized or unchannelized. A channelized T3 provides 28 T1 lines multiplexed into the T3. Each T1 line can be configured into one or more serial interface data channels.

Using the **no channelized** command, you can configure the T3 as a single, unchannelized serial interface data channel. You can configure this data channel to use all of the T3 bandwidth or a portion of it.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e5/5e_ct3.htm

Update to the Enhancements for the Cisco Voice Gateway 200

The Enhancements for the Cisco Voice Gateway 200 (Cisco VG200) feature provides the Cisco VG200 platform (also called CAG-VG200) with increased voice gateway feature parity to the Cisco 2600, Cisco 3600, and Cisco 3700 platforms. This update provides additional feature functionality on the Cisco VG200 platform.

The Cisco VG200 platforms provide the following default memory options: CAG-VG200—16 MB of Flash, 64 MB of DRAM

VPN Accelerator Module (VAM)

The VPN Acceleration Module (VAM) is a single-width acceleration module. It provides high-performance, hardware-assisted tunneling and encryption services suitable for virtual private network (VPN) remote access, site-to-site intranet, and extranet applications. It also provides platform scalability and security while working with all services necessary for successful VPN deployments — security, quality of service (QoS), firewall and intrusion detection, service-level validation, and management. The VAM off-loads IPSec processing from the main processor, thus freeing resources on the processor engines for other tasks.

The VAM provides hardware-accelerated support for multiple encryption functions:

- 56-bit Data Encryption Standard (DES) standard mode: Cipher Block Chaining (CBC)
- 3-Key Triple DES (168-bit)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5)
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122y/122ye/1229ye/12ye_vam.htm

VPN Encryption and Compression Module (AIM-VPN/EPII & AIM-VPN/HPII)

The VPN Encryption AIM provides hardware-based DES/3DES/AES and Compression services for Cisco 2691, Cisco 3660, Cisco 3725 and Cisco 3745 series routers. The Data Compression supports IPSec IPPCP and supports the industry standard LZS. For more information about configuring the virtual private network (VPN) encryption hardware advanced integration modules (AIM-VPN/EPII & AIM-VPN/HPII) and network modules, refer to the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftaimvpn.htm

WIC-1-B-U-V2

Beginning in this release, the model number for the existing WIC-1-B-U interface card for the Cisco 1700 series, Cisco 2600 series, and Cisco 3600 series is changing to WIC-1-B-U-V2.

In addition, this interface card will now be supported on the Cisco 1760, Cisco 2691, Cisco 3725 and Cisco 3745 beginning with this release.

New Software Features in Cisco IOS Release 12.2(13)T

The following new features are supported in Cisco IOS Release 12.2(13)T. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) feature adds support for the new encryption standard AES, with CBC (Cipher Block Chaining) Mode, to IP Security (IPSec).

The National Institute of Standards and Technology (NIST) has created AES, which is a new Federal Information Processing Standard (FIPS) publication that describes an encryption method. AES is a privacy transforms for IPSec and Internet Key Exchange (IKE) and has been developed to replace the Data Encryption Standard (DES). AES is designed to be more secure than DES: AES offers a larger key size, while ensuring that the only known approach for an intruder to decrypt a message is to try every possible key. AES has a variable key length—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_aes.htm

Analog DID (Direct Inward Dial)

Analog Direct Inward Dial (DID) is now supported on Cisco 1700 series routers.

Apollo Domain

The Apollo Domain networking protocol will no longer be offered after Cisco IOS Release 12.2. Apollo Domain commands will not appear in future releases of the Cisco IOS software documentation set.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

AppleTalk EIGRP

The AppleTalk Enhanced Interior Gateway Routing Protocol (Enhanced IGRP) will no longer be offered after Cisco IOS Release 12.2(13)T. AppleTalk EIGRP commands will not appear in future releases of the Cisco IOS software documentation set.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

ATM Multilink PPP Support on Multiple VCs

The ATM Multilink PPP Support on Multiple VCs feature supports the transport of real-time (voice) and other (data) traffic on Frame Relay and ATM virtual circuits (VCs).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftatmmlt.htm

ATM Policing by Service Category for SVC/SoftPVC

When configured, an ATM switch at the network side of a user-to-network (UNI) interface polices the flow of cells in the forward (into the network) direction of a virtual connection. These traffic policing mechanisms are known as usage parameter control (UPC). With UPC, the switch determines whether received cells comply with the negotiated traffic management values and takes one of the following actions on violating cells:

- Pass the cell without changing the cell loss priority (CLP) bit in the cell header.
- Tag the cell with a CLP bit value of 1.
- Drop (discard) the cell.

The ATM Policing by Service Category for SVC/SoftPVC feature enables you to specify which traffic to police, based on service category, on switched virtual circuits (SVCs) or terminating VCs on the destination end of a soft VC.

For more information on UPC, refer to the "Traffic and Resource Management" chapter in the *Guide to ATM Technology*.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/svc_upc.htm

ATM Subinterface MIB/Traps

This feature adds support for the monitoring of ATM and Frame Relay (FR) subinterface status using SNMP. New CLI commands allow the enabling or disabling of ATM and Frame Relay notifications (traps and informs), and provide an option for limiting the rate of notifications sent ("trap throttling").

Automatic Protection Switching (APS)

This feature allows switchover of packet-over-SONET (POS) circuits in the event of circuit failure and is often required when connecting SONET equipment to telco equipment.

Banyan VINES

The Banyan Virtual Network System (VINES) protocol will no longer be offered after Cisco IOS Release 12.2(13)T. Banyan VINES commands will not appear in future releases of the Cisco IOS software documentation set.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

BGP 4 MIB Support for per-Peer Received Routes

BGP 4 MIB Support for per-Peer Received Routes introduces a new table in the CISCO-BGP4-MIB that provides the capability to query (by using Simple Network Management Protocol [SNMP] commands) for routes that are learned from individual Border Gateway Protocol (BGP) peers.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftbgpmib.htm

BGP Policy Accounting

Border Gateway Protocol (BGP) policy accounting measures and classifies IP traffic that is sent to, or received from, different peers. Policy accounting is enabled on an input interface, and counters based on parameters such as community list, autonomous system number, or autonomous system path are assigned to identify the IP traffic.

Using the BGP **table-map** command, prefixes added to the routing table are classified by BGP attribute, autonomous system number, or autonomous system path. Packet and byte counters are incremented per input interface. A Cisco IOS policy-based classifier maps the traffic into one of eight possible buckets representing different traffic classes.

Using BGP policy accounting, you can account for traffic according to the route it traverses. Service providers (SPs) can identify and account for all traffic by customer and bill accordingly. Customers are billed appropriately for traffic that is routed from a domestic, international, or satellite source.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_bgppa.htm

Bisync-to-IP Conversion for Automated Teller Machines

The Bisync-to-IP Conversion for Automated Teller Machines feature enables customers to attach a binary synchronous communication (bisync) automated teller machine to a serial interface on a Cisco router running bisync-to-IP (BIP) protocol translation, and then to route the data over a TCP/IP network directly to an IP-based application host.

As of Cisco IOS Release 12.2(13)T you can use the **bstun peer-map-poll** command in global configuration mode to map the ATM state to polling. The default is to not map the peer state to polling. If you configure this command, BIP activates polling when the BIP tunnel becomes active and stops polling when the tunnel connection is terminated. When the peer state-to-polling is not mapped, BIP waits for the host to issue an "active" status message across the BIP tunnel before polling the ATM device and polling is stopped when an "inactive" status message is received across the tunnel or the tunnel connection is terminated.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftbipatm.htm

Call Admission Control for H.323 VoIP Gateways

Before the call admission control feature, gateways did not have a mechanism to gracefully prevent calls from entering when certain resources were not available to process the call. This causes the new call to fail with unreported behavior, and could potentially cause the calls that are in progress to have quality related problems.

This feature set provides the ability to support resource-based call admission control processes. These resources include system resources such as CPU, memory, and call volume, and interface resources such as call volume.

If system resources are not available to admit the call, two kinds of actions are provided: system denial (which busyouts all of T1 or E1) or per call denial (which disconnects, hairpins, or plays a message or tone). If the interface-based resource is not available to admit the call, the call is dropped from the session protocol (such as H.323).

This feature was previously released in Cisco IOS Release 12.2(4)T on the Cisco 2600 and Cisco 3600 routers, and Cisco MC3810 multiservice concentrators. This release is porting the feature into the IAD2420 platform.

Call Release Source Reporting in Gateway-Generated Call Accounting Records

The Call Release Source Reporting in Gateway-Generated Call Accounting Records feature enables you to track the source of call release in a Voice over IP (VoIP) network. This call release information defines whether a call was released by the calling or called party or by an internal or external source.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_crsr.htm

CEF and Distributed CEF Switching for IPv6

Cisco Express Forwarding for IPv6 (CEFv6) is advanced, Layer 3 IP switching technology for the forwarding of IPv6 packets. Distributed CEF for IPv6 (dCEFv6) performs the same functions as CEFv6 but for distributed architecture platforms such as the Cisco 12000 series Internet routers and the Cisco 7500 series routers. dCEFv6 and CEFv6 function the same and offer the same benefits as dCEFv4 and CEFv4—network entries that are added, removed, or modified in the IPv6 Routing Information Base (RIB), as dictated by the routing protocols in use, are reflected in the Forwarding Information Bases (FIBs), and the IPv6 adjacency tables maintain Layer 2 next-hop addresses for all entries in each FIB.

CEFv6 was introduced in Cisco IOS Release 12.2(13)T for nondistributed architecture platforms, such as the Cisco 7200 series routers. dCEFv6 was introduced in Cisco IOS Release 12.0(21)ST for the Cisco 12000 series Internet routers, and was then integrated into Cisco IOS Release 12.2(13)T and later releases for other distributed architecture platforms, such as the Cisco 7500 series routers.

In Cisco IOS Release 12.0(21)ST, dCEFv6 included support for IPv6 addresses and prefixes. In Cisco IOS Release 12.2(13)T or later releases, dCEFv6 and CEFv6 were enhanced to include support for separate FIBs for IPv6 global, site-local, and link-local addresses.

Cisco Conferencing and Transcoding for Voice Gateway Routers

The feature enables voice conferencing to take place among conferees at small, remote branch offices or distributed sites using local resources, without calls having to traverse the company WAN to the central site that supports such services.

The feature also provides transcoding at the remote site. Different IP telephony devices support different codecs and, for communications to be enabled between them, transcoding is required. The feature provides transcoding at the remote site, without having to access transcoding services at the central site.

To provide these services, the feature takes advantage of unused DSP resources on a network module in an already existing small or midsize Cisco router at the remote site. The collection of DSP resources so made available is called a DSP farm. The DSP farm is managed by Cisco CallManager, the software-based call-processing component of the Cisco IP telephony solution, at a central office or branch office.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftdsp.htm

Cisco IOS Software Feature Removal

This feature permanently removes selected legacy features (or components) from the Cisco IOS code. These features will not be available in future releases of Cisco IOS software.

The features that have been removed in the 12.2(13)T release are as follows:

- AppleTalk EIGRP
- Apollo Domain
- Banyan VINES
- Exterior Gateway Protocol (EGP)
- HP Probe
- Interior Gateway Routing Protocol (IGRP)
- Next Hop Resolution Protocol (NHRP) for IPX
- NetWare Link Services Protocol (NLSP)
- Simple Multicast Routing Protocol (SMRP) for AppleTalk
- Xerox Network Systems (XNS)

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

Cisco IOS Telephony Service (ITS) Version 2.02

The new feature for Cisco IOS Telephony Service (ITS) Version 2.02 is an increase in directory numbers from 192 to 288 for the following platforms:

- Cisco 2691 router
- Cisco 3640 routers
- Cisco 3660 routers
- Cisco 3725 routers
- Cisco 3745 routers

The *Cisco IOS Telephony Service V2.02 Feature Guide* is located at the following location:

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_feature_guides_list.html

Cisco Mobile Networks—Asymmetric Link

An asymmetric link environment such as satellite communications, with a separate uplink and downlink, provides challenges for the mobile router and foreign agent.Because each unidirectional link provides only one way traffic, the inherent mapping in the foreign agent of the return path to the mobile router for incoming messages does not apply. The Cisco Mobile Networks—Asymmetric Link feature solves this problem by extending the use of mobile networks to networks where the mobile router has unidirectional links to the foreign agent. The foreign agent is able to transmit packets back to the mobile router over a different link than the one on which it receives packets from the mobile router.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/asymmetr.htm

Cisco Mobile Networks—Dynamic Network Support

The Cisco Mobile Networks feature enables a mobile router and its subnets to be mobile and maintain all IP connectivity, transparent to the IP hosts connecting through this mobile router. Previously, this feature was a static network implementation that supported stub routers only.

Cisco IOS Release 12.2(13)T introduces dynamic network support, which means that the mobile router dynamically registers its mobile networks to the home agent, which reduces the amount of configuration required at the home agent. For example, if a home agent supports 2000 mobile routers, the home agent does not need 2000 configurations but only a range of home IP addresses to use for the mobile routers.This registration results in minimal configuration on the home agent making administration and set up easier.

Cisco Survivable Remote Site Telephony Service V2.02

The new feature for Cisco Survivable Remote (SRS) Telephony V2.02 is Unity Voice Mail integration, which introduces six new commands:

- **pattern direct**
- **pattern ext-to-ext busy**
- pattern ext-to-ext no-answer
- **pattern trunk-to-ext busy**
- **pattern trunk-to-ext no-answer**
- **vm-integration**

For further information, see *Cisco IOS Telephony Service V2.02* at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/srs/index.htm

Class-Based RTP and TCP Header Compression

Real-time Transport Protocol (RTP) or Transmission Control Protocol (TCP) IP header compression is typically configured at the interface level. However, this feature now allows you to configure RTP or TCP IP header compression on a per-class basis, when a class in configured within a policy map. Policy maps are created using the Modular Quality of Service Command-Line Interface (MQC).

Thus, this feature extends the functionality of the MQC and allows you to configure and fine-tune IP header compression at a more granular level.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/fthdrcmp.htm

Clearable SIP-UA Statistics

This feature provides the ability to clear all Session Initiation Protocol (SIP) statistics counters that are displayed by the **show sip-ua statistics** command, which includes response, traffic and retry statistics. Prior to the implementation of the new feature, SIP counters could be cleared only by reloading or resetting the router. The new feature enhances both trouble-shooting and statistical analysis efforts by clearing SIP counters without reloading or resetting the router.

The new feature includes the following functionality:

- Provides an alternate, convenient way to clear statistics counters through the CLI
- Provides separate views of CLI and SNMP statistics counters
- Provides a timestamp indicating **clear sip-ua statistics** command activity to assist in reconciling CLI and SNMP counter polls

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftshadow.htm

Committed Access Rate (CAR)

Committed Access Rate (CAR) can rate limit traffic based on certain matching criteria, such as incoming interface, IP Precedence, or IP access list.

Connection-Oriented Media (Comedia) Enhancements for SIP

This feature provides the following functionality to symmetric Network Address Translation (NAT) traversal:

- Allows the Cisco gateway to check the media source of incoming Real-time Transport Protocol (RTP) packets.
- Allows the endpoint to advertise its presence inside or outside of NAT.

The new feature implements one of many possible SIP solutions to address problems with different NAT types and traversals.With the Connection-Oriented Media (Comedia) Enhancements for SIP feature, the gateway can open an RTP session with the remote end and then update or modify the existing RTP session's remote address and port **(raddr:rport)** with the source address and port of the actual media packet received after passing through NAT.

Dial-Peer Support for Data Calls

The Dial-Peer Support for Data Calls feature enables the configuration and order assignment of dial peers so that a gateway can identify incoming calls as voice or data. The feature provides a unified call processing model that is scalable for voice and data calls through dial-peer provisioning. The feature also enables the capability of assigning separate number ranges for voice or data calls so that the calls will have the same preference level of matching.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftconcrt.htm

Distributed IPv6 for Cisco IOS software

This feature provides distributed CEF switching support for IPv6 on the Cisco 7500 platforms.

DLR Enhancements: PGM RFC-3208 Compliance

In compliance with RFC 3208, the DLR Enhancements feature adds off-tree designated local repairer (DLR) support and redirecting poll response (POLR) capability for upstream DLRs to the Cisco implementation of Pragmatic General Multicast (PGM).

Dual Serial Line Management to Interface Lucent 5ESS

This feature is a part of the Cisco IOS Telco Feature Set, a bundle of applications specific to the data communications network (DCN) environment. Specifically, this feature supports X.25-to-TCP protocol translation, and provides dual serial interfaces to preserve the redundancy and monitoring capability available from SCC0 and SCC1 links on a Lucent 5ESS switch in the DCN network.

Dynamic Multipoint VPN (DMVPN)

The Dynamic Multipoint VPN (DMVPN) feature combines GRE tunnels, IPSec encryption, and NHRP routing to provide users an ease of configuration via crypto profiles, which override the requirement for defining static crypto maps, and dynamic discovery of tunnel endpoints.

This feature relies on the following two Cisco technologies—NHRP and mGRE Tunnel Interface.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftgreips.htm

Dynamic Subscriber Bandwidth Selection

The Dynamic Subscriber Bandwidth Selection (DBS) feature enables wholesale service providers to sell different classes of service to retail service providers by controlling bandwidth at the ATM Virtual Circuit (VC) level. ATM Quality of Service (QoS) parameters from the subscriber domain are applied to the ATM PVC on which a PPPoE or PPPoA session is established.

Using DBS you can set the ATM permanent virtual circuit (PVC) traffic shaping parameters to be dynamically changed based on the RADIUS profile of a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) user logging in on the PVC. If the user is the first user on that PVC, then the RADIUS profile values override the default values of the PVC. If users already exist on the PVC, then the new value overrides the existing configuration only if it is higher than the existing value. If multiple PPPoE sessions are allowed on a subscriber VC, then the highest peak cell rate (PCR) and sustainable cell rate (SCR) of all the sessions is selected as the PCR and SCR of the VC.

You can apply DBS QoS parameters per user as well as per domain. If you apply DBS QoS parameters under a domain profile, all users in that profile are assigned the same DBS QoS parameters. These parameters are assigned to the RADIUS profile for that domain. You can also apply distinctive DBS QoS parameters via the RADIUS user profile.

Traffic shaping parameters can be locally configured by IOS CLI in VC-mode, VC-class, range mode, or PVC-in-range mode. These parameters have a lower priority and are overridden by the shaping parameters specified in the domain service profile. Traffic shaping parameters that are CLI configured at the VC class interface or subinterface level are treated as the default QoS parameters for the PVCs to which they apply. These parameters are overridden by the domain service profile QoS parameters of the domain the user is logged in to. If no VC class is configured, the default is the unspecified bit rate (UBR).

When a network access server (NAS) sends a domain authorization request and receives an affirmative response from the RADIUS server, this response may include a "QoS-management" string via vendor-specific attribute (VSA) 26 for QoS management in the NAS. The QoS management values are configured as part of the domain service profile attributes on the RADIUS server. These values contain PCR and SCR values for a particular user or domain. If the QoS specified for a domain or user cannot be applied on the PVC that the session belongs to, the session is not established.

Changing PVC traffic parameters because of new simultaneous PPPoE sessions on the PVC does not cause existing PPPoE sessions that are already established to disconnect. Changing domain service profile QoS parameters on the RADIUS server does not cause traffic parameters to automatically change for PVCs that have existing sessions.

When you enter the **dbs enable** or **no dbs enable** commands to configure or unconfigure DBS, existing sessions are not disconnected. If you have a session that has been configured for DBS and you configure the **no dbs enable** command on a VC, additional sessions that are configured will display DBS configured QoS values until the first new session is up. After the first session is brought up, the VC has default and locally configured values. If you configure the **dbs enable** command after multiple sessior are already up on the VC, all sessions on that VC have DBS QoS parameters.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftdbs.htm

Enhanced Features for Local and Advanced Voice Busyout

This feature introduces 2 new commands, **busyout monitor gatekeeper** and **busyout action graceful**. The **busyout monitor gatekeeper** command busies out the gatekeeper if the gateway loses connection to the primary gatekeeper and removes the busyout state when the gateway restores connection to the primary or backup gatekeeper. The **busyout action graceful** command controls the busyout behavior that is triggered by the **busyout monitor** command. This command busies out the voice port immediately if the busyout behavior is triggered but if there is an active call on this voice port it will wait until the call is over.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_lavbo.htm

Enhanced ITU-T G.168 Echo Cancellation

This feature provides an alternative to the default, Cisco proprietary 32-millisecond G.165 echo canceller (EC). The new extended echo canceller provides improved performance for trunking gateway applications and provides a configurable tail length that supports up to 64 milliseconds (ms) of echo cancellation. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftecho.htm

Enhanced Packet Marking

The Enhanced Packet Marking feature allows you to map and convert the marking of a packet from one value to another (for example, the Precedence value can be mapped to the equivalent Class of Service (CoS) value) by using a kind of conversion chart called a table map.

The table map establishes an equivalency from one value to another. For example, the table map can map the CoS value of a packet to the Precedence or differentiated services code point (DSCP) value of the packet. For networks using MPLS, the MPLS EXP value can be mapped to the QoS group value, which can then be mapped to the Precedence or DSCP value of the packet. This value mapping can be propagated for use on the network, as needed. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftenpkmk.htm

Enhancements for the Cisco Voice Gateway 200

The Enhancements for the Cisco Voice Gateway 200 (VG200) feature provides the Cisco VG200 platform with increased voice gateway feature parity to the Cisco 2600, Cisco 3600, and Cisco 3700 platforms. This update provides additional feature functionality on the Cisco VG200 platform. Refer to the following document for additional information:

Exterior Gateway Protocol (EGP)

The Exterior Gateway Protocol (EGP) will no longer be offered after Cisco IOS Release 12.2(13)T. EGP commands will not appear in future releases of the Cisco IOS software documentation set.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

File System Check and Repair for PCMCIA ATA Disks

This feature introduces a File-System-Check (fsck) utility in Cisco IOS software for FAT file systems on PCMCIA disks. The utility performs functions such as checking the boot sector and partition table, checking file and directory structure, reclaiming unused disk space, and updating the FAT file structure. Prior to the introduction of this utility, corrupt files could not be removed from ATA disks using the Cisco IOS CLI. This utility is run using the **fsck** privileged EXEC mode command.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_fsck.htm

Frame Relay PVC Bundles with IP and MPLS QoS Support

Frame Relay PVC bundles allow you to associate a group of Frame Relay permanent virtual circuits (PVCs) with a single next-hop address. When Frame Relay PVC bundles are used with IP, packets are mapped to specific PVCs in the bundle on the basis of the precedence value or differentiated services code point (DSCP) settings in the type of service (ToS) field of the IP header. Each packet is treated differently according to the QoS configured for each PVC.

Frame Relay PVC bundles with MPLS QoS support extends Frame Relay PVC bundle functionality to support the mapping of Multiprotocol Label Switching (MPLS) packets to specific PVCs in the bundle. MPLS packets are mapped to PVCs according to the settings of the experimental (EXP) bits in the MPLS packet header.Waiting for information.

Frame Relay Queueing and Fragmentation at the Interface

The Frame Relay Queueing and Fragmentation at the Interface feature introduces support for low-latency queueing (LLQ) and FRF.12 end-to-end fragmentation on a Frame Relay interface. This new feature simplifies the configuration of low-latency, low-jitter quality of service (QoS) by enabling the queueing policy and fragmentation configured on the main interface to apply to all permanent virtual circuits (PVCs) and subinterfaces under that interface. Before the introduction of this feature, queueing and fragmentation had to be configured on each individual PVC. Subrate shaping can also be configured on the interface.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/frfrintq.htm

H.323 Call Redirection Enhancements

The user-to-user information element (UUIE) of the Facility message is used primarily for call redirection. The UUIE contains a field, facilityReason, that indicates the nature of the redirection. The H.323 Call Redirection Enhancements feature adds support for two of the reasons: routeCallToGatekeeper and callForwarded. It also provides a non-standard method for using the Facili message to effect call transfer.

This feature was previously released in Cisco IOS Release 12.2(2)T on Cisco 1700, Cisco 2600 series, Cisco 3600 series, Cisco MC3810, Cisco AS5300, Cisco uBR924 platforms. This release is porting the feature into the IAD2420 platform.

H.323 Dual Tone Multifrequency Relay Using Named Telephone Events

The NTE method of DTMF relay was originally available on Cisco gateways only for Session Initiation Protocol (SIP) and Media Gateway Control Protocol (MGCP) gateways. The H.323 DTMF Relay Using Named Telephone Events (NTE) feature adds support for this method for H.323 gateways.

Cisco H.323 gateways advertise capabilities using the H.245 capabilities messages. By default, they advertise that they can receive all DTMF relay modes. If the capabilities of the remote gateway do not match, the Cisco H.323 gateway transmits DTMF tones as in-band voice. Configuring DTMF relay on the Cisco H.323 gateway sets preferences for how the gateway handles DTMF transmission. If multiple methods are configured, the priority is as follows:

- Cisco RTP
- RTP NTE
- H.245 signal
- H.245 alphanumeric

In addition to support for NTE, the H.323 DTMF Relay Using NTE feature provides support for asymmetrical payload types. Payload types can differ between local and remote endpoints. Therefore, the Cisco gateway can transmit one payload type value and receive a different payload type value.

This feature was previously released in Cisco IOS Release 12.2(11)T on Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms. This release is porting the feature into the IAD2420 platform.

H.323 (Gateway) Support

Support for H.323 Version 2 Gateway functionality is added to the Cisco IAD2420 series of integrated access devices (IADs). This support provides the Cisco IAD2420 IAD with more market opportunities than when the IAD only supported MGCP and SGCP call control protocols.

The Cisco IAD2420 IAD with 16 FXS analog ports delivers local voice and data service using VoIP in an Ethernet To The Building (ETTx) application. It aggregates the voice traffic from multiple tenants and transports it to an Ethernet switch, such as the Cisco 2950, over the Ethernet link. The built-in WAN interface (either a T1, ADSL or SHDSL module) is not used when using the IAD2420-16FXS.

H.323 Redundant Zone Support

The Redundant H.323 Zone Support feature allows users to configure multiple gatekeepers to service the same zone or technology prefix. This feature can be used with the Gateway Support for Alternate Gatekeepers feature, which allows a user to configure a gateway to point to two gatekeepers (one as the primary and the other as the alternate). Together, these features allow a user to configure a Cisco gateway to send location requests (LRQs) to two or more Cisco gatekeepers---one as a primary and the others as back up gatekeepers.

This feature was previously released in Cisco IOS Release 12.1(1)T on Cisco 2600 series, Cisco 3600 series, Cisco MC3810, Cisco AS5200, Cisco AS5300, and Cisco AS5800 platforms. This release is porting the feature into the Cisco IAD2420 platform.

H.323 Scalability and Interoperability Enhancements

The Cisco H.323 Scalability and Interoperability Enhancements feature upgrades the Cisco H.323 Gatekeeper and Cisco H.323 Gateway to comply with H.323 Version 3. The enhancements in this release include support for mandatory H.323 Version 3 elements in the gateway, support for H.225 call signalling over UDP, and address resolution using border elements.

For gatekeeper support, this feature was previously released in Cisco IOS Release 12.2(4)T on Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco MC3810, Cisco AS5850, and Cisco 7200 series platforms. For gateway support, this feature was previously released in Cisco IOS Release 12.2(4)T on Cisco 1700, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5850, Cisco uBR900 series, and Cisco uBR924 platforms. This release is porting the feature into the IAD2420 platform.

H.323 Support for Virtual Interfaces

The H.323 Support for Virtual Interfaces feature allows users to configure the IP address of the gateway, so that the IP address include in the H.323 packet is deterministic and consistently indicates the same address for the source.

In previous releases of the Cisco IOS software, the source address included in the H.323 packet could vary depending on the protocol (RAS, H.225, H.245, or RTP). This makes it difficult to configure firewall applications to work with H.323 messages.

The H.323 Support for Virtual Interfaces feature addresses that difficulty by allowing the user to explicitly configure an IP address to be used for all protocols

This feature was previously released in Cisco IOS Release 12.1(2)T on Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, and Cisco uBR924 platforms. This release is porting the feature into the IAD2420 platform.

HP Probe

The HP Probe feature will no longer be offered after Cisco IOS Release 12.2(13)T. HP Probe commands will not appear in future releases of the Cisco IOS software documentation set.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

Interim Local Management Interface (ILMI)

The Interim Local Management Interface (ILMI) is a protocol defined by the ATM Forum for setting and capturing physical layer, ATM layer, virtual path, and virtual circuit parameters on ATM interfaces. ILMI uses simple network management protocol (SNMP) messages without User Datagram Protocol (UDP) and IP, and organizes managed objects into the following four management information bases (MIBs).

Interim-Interswitch Signaling Protocol (IISP)

The Interim-Interswitch Signalling Protocol (IISP) defines a static routing protocol (using manually configured prefix tables) for communication between ATM switches. IISP provides support for switched virtual circuits (SVCs) on ATM switches that do not support the Private Network-to-Network Interface (PNNI) protocol.

Interim Update at Call Connect

With this feature, Cisco IOS software generates and sends an additional updated interim accounting record to the accounting server when a call leg is connected. All attributes (for example, h323-connect-time and backward-call-indicators) available at the time of call connection are sent through this interim updated accounting record. Refer to the following document for additional information:

Interior Gateway Routing Protocol (IGRP)

The Interior Gateway Routing Protocol (IGRP) will no longer be offered after Cisco IOS Release 12.2(13)T. IGRP commands will not appear in future releases of the Cisco IOS software documentation set.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

IP Event Dampening

Interface state changes occur when interfaces are administratively brought up or down or if an interface changes state. When an interface changes state or flaps, routing protocols are notified of the status of the routes that are affected by the change in state. Every interface state change requires all affected devices in the network to recalculate best paths, install or remove routes from the routing tables, and then advertise valid routes to peer routers. An unstable interface that flaps excessively can cause other devices in the network to consume substantial amounts of system processing resources and cause routing protocols to lose synchronization with the state of the flapping interface.

The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping. Dampening an interface removes the interface from the network until the interface stops flapping and becomes stable. Configuring the IP Event Dampening feature improves convergence times and stability throughout the network by isolating failures so that disturbances are not propagated, which reduces the utilization of system processing resources by other devices in the network and improves overall network stability.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftipevdp.htm

IPSec NAT Transparency

Before the introduction of the IPSec NAT Transparency feature, a standard IPSec VPN tunnel would not work if there were one or more NAT or PAT points in the delivery path of the IPSec packet. This feature introduces support for IPSec traffic to travel through NAT or PAT points in the network by encapsulating IPSec packets in a User Datagram Protocol (UDP) wrapper, thereby, allowing remote access users to build IPSec tunnels to home gateways.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftipsnat.htm

IPSec Passive Mode

The IPSec Passive mode feature allows users to configure an intermediate mode—IPSec passive mode—that enables routers within an existing network to accept encrypted and unencrypted data. The routers will also attempt to negotiate an encrypted session when sending data, but they will send the data in unencrypted form as necessary.

IPSec passive mode is valuable for users who wish to migrate existing networks to IPSec because they no longer have wait for all routers to deploy IPSec; that is, all routers will continue to interact with routers that will encrypt data (that have been upgraded with IPSec) and routers that have yet to be upgraded.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftpasips.htm

Note Because a router in IPSec passive mode is insecure, make sure that no routers are accidentally left in this mode after upgrading a network.

IPv6 ADSL and Dial Deployment Support

The IPv6 ADSL and Dial Deployment Support feature adds support for IPv6 prefix pools, and per-user IPv6 Radius attributes. It further enables deployment of IPv6 in DSL and dial access environments. This feature provides the extensions that make large scale IPv6 access possible for IPv6 environments, including IPv6 Radius attributes, stateless address configuration on PPP links, per-user static routes, and access lists (ACLs). Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ipv6/index.htm

IPv6 Extended Access Control Lists

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, standard IPv6 access control list (ACL) functionality is used for basic traffic filtering functions—traffic filtering is based on source and destination addresses, inbound and outbound to a specific interface, and with an implicit deny statement at the end of each access list (functionality similar to standard ACLs in IPv4). IPv6 ACLs are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode.

In Cisco IOS Release 12.2(13)T or later releases, and 12.0(23)S, the standard IPv6 ACL functionality is extended to support—in addition to traffic filtering based on source and destination addresses—filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4). IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. (Configuring the **ipv6 access-list** command places the router in IPv6 access list configuration mode, from which permit and deny conditions can be set for the defined IPv6 ACL.)

IPv6 Quality of Service

This feature provides for the application of all the Differentiated Services (DiffServ) QoS features to IPv6 packets. Specific QoS features include packet classification, traffic shaping, traffic policing, packet marking, and Drop based on Weighted Random Early Detect (WRED) on all applicable interfaces.

IPv6 RIP Enhancements

The IPv6 RIP Enhancements feature adds support for a separate IPv6 RIP routing table, the ability to delete routes from the IPv6 RIP routing table, and the ability to set route tags. The holddown timer default is now set to zero, and a maximum number of parallel routes can be configured.

IS-IS HMAC-MD5 Authentication

The IS-IS HMAC-MD5 Authentication feature adds an HMAC-MD5 digest to each Intermediate System-to-Intermediate System (IS-IS) protocol data unit (PDU). HMAC is a mechanism for message authentication codes (MAC) using cryptographic hash functions. The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing messages from being injected into the network routing domain.

IS-IS has five packet types: link-state packet (LSP), LAN Hello, Serial Hello, complete sequence numbe PDU (CSNP), and partial sequence number PDU (PSNP). The IS-IS HMAC-MD5 authentication or th cleartext password authentication can be applied to all five types of PDU. The authentication can be enabled on different IS-IS levels independently. The interface-related PDUs (LAN Hello, Serial Hello, CSNP and PSNP) can be enabled with authentication on different interfaces, with different levels and different passwords.

The HMAC-MD5 mode cannot be mixed with the clear text mode on the same authentication scope (LSP or interface). However, administrators can use one mode for LSP and another mode for some interfaces, for example. If mixed modes are intended, different keys should be used for different modes in order not to compromise the encrypted password in the PDUs.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftismd5.htm

L2TP Extended Failover

The L2TP Extended Failover feature extends Layer 2 Tunneling Protocol (L2TP) failover to occur if during tunnel establishment, a router receives a Stop-Control-Connection-Notification (StopCCN) message from its peer or during session establishment, a router receives a Call-Disconnect-Notify (CDN) message from its peer. In either case, the router selects an alternate peer to contact. This is in addition to the existing failover caused by excessive retransmission of Start-Control-Connection-Reply (SCCRQ) messages that indicate there is no response from the peer.

L2TP Extended Failover results in better load distribution and prevents congestion at a tunnel terminator by allowing the busy tunnel terminator to inform the tunnel initiator that it should try another tunnel terminator.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftl2tpef.htm

L2TP Redirect

The L2TP Redirect feature allows an L2TP network server (LNS) participating in Stack Group Bidding Protocol (SGBP) to send a redirect message to the L2TP access concentrator (LAC) if another LNS wins the bid. The LAC will then reinitiate the call to the newly redirected LNS. The feature provides two purposes:

- Allows the user to have more evenly load-balanced sessions among a stack of LNSs
- For multilink calls over Layer 2 Tunneling Protocol (L2TP), eliminates the need for multiple hops

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftl2tpmr.htm

Low Latency Queueing (LLQ) for IPSec

Low Latency Queueing (LLQ) for IPSec encryption engines helps reduce packet latency by introducing the concept of queueing before crypto engines. Prior to this, the crypto processing engine gave data traffic and voice traffic equal status. Administrators now designate voice traffic as priority. Data packets arriving at a router interface are directed into a data packet inbound queue for crypto engine processing. This queue is called the best effort queue. Voice packets arriving on a router interface are directed into a priority packet inbound queue for crypto engine processing. This queue is called the priority queue. The crypto engine undertakes packet processing in a ratio favorable for voice packets. Voice packets are guaranteed a minimum processing bandwidth on the crypto engine.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/llqfm.htm

LZ Software with Hardware Encryption

Before the LZ Software with Hardware Encryption feature was introduced, compression was not supported with the VPN encryption hardware advanced integration module (AIM) and network module (NM); that is, a user had to remove the VPN module from the router and run software encryption with software compression. This feature enables all VPN modules to support LZ compression in software when the VPN module is in Cisco 2600 and Cisco 3600 series routers, thereby, allowing users to configure and compress 2 128Kb/sec streams.

Manual Certificate Enrollment (TFTP and Cut-and-Paste)

The Manual Certificate Enrollment (TFTP and Cut-and-Paste) feature allows users to generate a certificate request and accept Certificate Authority (CA) certificates as well as the router's certificates; these tasks are accomplished via a TFTP server or manual cut-and-paste operations. Users may wish to utilize TFTP or manual cut-and-paste enrollment in the following situations:

- Their CA does not support Simple Certificate Enrollment Protocol (SCEP) (which is the most commonly used method for sending and receiving requests and certificates)
- A network connection between the router and CA is not possible (which is how a router running Cisco IOS software obtains it certificate)

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmancrt.htm

Media Forking

Media Forking allows the gateway to create multiple streams (or forks) of media associated with a single call and send those streams to multiple destinations, which may include voice portals with speech recognition. Only the original media stream is bidirectional. Additional branches are unidirectional (transmit only), so additional participants are able to hear only the originating caller and not each other. Each media stream is independently configured and can be a variation of voice only, named telephone event (NTE) only, or voice plus NTE media stream.The content of the media stream is specified in the signaling when the media stream is established.

Although there can be more than one media destination, there is only one signaling destination, which might be the voice portal. The call leg that was originally signaled (for instance, from the originating gateway to the voice portal) is maintained for the life of the session. The media destinations are independent of the signaling destination, so media forks can be added and removed dynamically. The local telephony call leg must be maintained, and up to four media forks, including the destination of the original call, are supported. Fax calls are not supported on any media streams (including the original) when multiple forks are requested. No media forks can be created for a fax call session.

MGCP 1.0 and TGCP 1.0 Profiles

This feature implements the following MGCP protocols on the supported Cisco media gateways:

- MGCP 1.0 (RFC 2705)
- Network-based Call Signaling (NCS) 1.0, the MGCP 1.0 profile for residential gateways (RGWs)
- Trunking Gateway Control Protocol (TGCP) 1.0, the MGCP 1.0 profile for trunking gateways (TGWs)

MGCP1.0 is a protocol for the control of Voice over IP (VoIP) calls by external call-control elements known as media gateway controllers (MGCs) or call agents (CAs). It is described in the informational RFC 2705, published by the Internet Society.

PacketCable is an industry-wide initiative for developing interoperability standards for multimedia services over cable facilities using packet technology. PacketCable developed the NCS and TGCP protocols, which contain extensions and modifications to MGCP while preserving basic MGCP architecture and constructs. NCS is designed for use with analog, single-line user equipment on residential gateways, while TGCP is intended for use in VoIP-to-PSTN trunking gateways in a cable environment. To meet European cable requirements and equipment characteristics, the EuroPacketCable working group has adapted PacketCable standards under the name *IP Cablecom*.

The 'cmiHaRegMobilityBindingTable' is augmented from 'haMobilityBindingTable' of the RFC2006-MIB (MIP MIB) to provide the NAI information.

2. HA redundancy feature.

Scalar objects have been added to MIB to monitor the message exchanges between peer home agents. These objects are under the 'cmiHaRedun' subtree of the MIB.

3. Performance monitoring.

There are scalar objects under 'cmiHaReg' subtree which gives statistics about the registration processing rate at home agent. Distinction is made between registration requests authenticated locally and those authenticated at the AAA server. There are scalar objects under the 'cmiMaReg' subtree which give statistics about the rate at which registration requests are received at the mobility agent (HA or FA).

Mobile IP—NAT Detect

The basic purpose of Network Address Translation (NAT) is to take traffic from the internal network and present it to the Internet as if it were coming from a single device having only one IP address. Traditional Mobile IP tunneling is incompatible with NAT. The Mobile IP—NAT Detect feature allows the home agent to tunnel traffic to Mobile IP clients with private IP addresses behind a NAT-enabled device. The home agent is capable of detecting a registration request traversing a NAT-enabled device and applying the appropriate tunnel to reach the Mobile IP client.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftnatrav.htm

Mobile IP—Private Addressing Support

The Mobile IP—Private Addressing Support feature allows the use of private IP addresses for mobile nodes. Enhancements have been made to the foreign agent to allow it to distinguish between mobile nodes using the same private home address, but with different home agents.

When a mobile node successfully registers with a foreign agent, a tunnel is set up between the foreign agent and the home agent. When a packet is received by the foreign agent for the mobile node, the foreign agent will identify which mobile node to route the packet to based on the address of the mobile node, as well as the home agent from which the packet came.

Mobile IP—Support for FA Reverse Tunneling

The Mobile IP—Support for Foreign Agent Reverse Tunneling feature prevents packets sent by a mobile node from being discarded by routers configured with ingress filtering by creating a reverse tunnel between the foreign agent and the home agent.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_farev.htm

Modular QoS CLI (MQC)-Based Frame-Relay Traffic Shaping

The Modular Quality of Service (QoS) Command Line Interface (CLI)-Based Frame-Relay Traffic Shaping feature provides users the ability to configure Frame Relay traffic shaping (FRTS) using Modular Quality of Service (QoS) Command Line Interface (CLI) commands. Modular QoS CLI is known as MQC.

Modular QoS CLI (MQC) Three-Level Hierarchical Policer

Earlier Cisco IOS traffic policing features allowed you to configure traffic policing at two levels of policy map hierarchies; the top level and a secondary level.

The Modular QoS CLI (MQC) Three-Level Hierarchical Policer extends the traffic policing functionality by allowing you to configure traffic policing at *three* levels of policy map hierarchies; a top level, a secondary level, and a third level. Traffic policing may be configured at any or all of these levels, depending on the needs of your network. The feature is configured using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Configuring traffic policing in a three-level hierarchical structure provides a greater degree of granularity for traffic policing.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft3level.htm

Modular QoS CLI (MQC) Unconditional Packet Discard

This feature allows customers to classify traffic matching certain criteria and then configure the system to unconditionally discard any packets matching that criteria. This feature is configured using the Modular Quality of Service Command-Line Interface (MQC) feature.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftcbdrp.htm

MPLS DiffServ Tunneling Modes

MPLS DiffServ Tunneling Modes allows service providers to manage the QoS that a router will provide to an MPLS packet in an MPLS network. MPLS DiffServ Tunneling Modes conforms to the IETF draft standard for Uniform, Short Pipe, and Pipe modes, and to Cisco-defined extensions for scalable CLI management of those modes at customer edge, provider edge, and core routers.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftdtmode.htm

MPLS Label Distribution Protocol (LDP) MIB

Multiprotocol label switching (MPLS) is a packet forwarding technology that uses a short, fixed-length value called a label in packets to determine the next hop for packet transport through an MPLS network by means of label switching routers (LSRs).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ldpmib13.htm

MPLS Virtual Private Networks

The Virtual Private Network (VPN) feature for Multiprotocol Label Switching (MPLS) allows a Cisco IOS network to deploy scalable IPv4 Layer 3 VPN backbone services.

This feature was originally introduced in 12.0(5)T. This release introduces the command.

MGCP Model

MGCP bases its call control and intelligence in centralized *call agents*, also called media gateway controllers. The call agents issue commands to simple, low-cost endpoints, which are housed in media gateways (MGs), and the call agents also receive event reports from the gateways. MGCP messages between call agents and media gateways are sent with Internet Protocol over User Datagram Protocol (IP/UDP).

The MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles feature provides protocols for RGWs and TGWs, which sit at the border of the packet network to provide an interface between traditional, circuit-based voice services and the packet network. Residential gateways offer a small number of analog line interfaces, while trunking gateways generally manage a large number of digital trunk circuits.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_24mg1.htm

MGCP Gateway Support for the Bind Command

Previous Media Gateway Control Protocols (MGCP) implementation did not allow the assignment of particular IP addresses for sourcing MGCP commands and media packets, which could cause firewall and security problems. With this feature, you can configure interfaces on which control and media packets can be exchanged. This new functionality allows you to separate signaling from voice by binding control (MGCP signaling) and media (Real-Time Transport Protocol, or RTP voice, fax, and modem) to specific gateway interfaces. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftxbind.htm

Mobile IP—Challenge/Response Extensions

The Mobile IP—Challenge/Response Extensions feature enables a foreign agent to authenticate a mobile node by sending mobile foreign challenge extensions (MFCE) and mobile node-AAA authentication extensions (MNAE) to the home agent in registration requests. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_chext.htm

Mobile IP—Fastswitching Support on Foreign Agent

The Mobile IP—Fastswitching Support on Foreign Agent feature enables packets to be fast switched from the foreign agent both in the direction of the mobile node and through the reverse tunnel. In the direction of the mobile node, packets will be properly fast-switched for global IP addresses. However, this feature does not support fast-switching to mobile nodes using private home addresses.

Fast-switching packets through the reverse tunnel is achieved by intercepting packets before cache lookup and dynamically switching them through the correct tunnel interface.

Mobile IP—Generic NAI Support and Home Address Allocation

The Mobile IP—Generic NAI Support and Home Address Allocation feature allows a mobile node to be identified by using a network access identifier (NAI) instead of an IP address (home address). The NAI is a character string similar to an email address in that it is formatted as either *user* or *user@realm* but it need not be a valid e-mail address.

The original purpose of the NAI was to support roaming between dialup ISPs. With the NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each realm.

These services are also valuable for mobile nodes using Mobile IP when the nodes are attempting to connect to foreign domains with AAA servers. The mobile node can identify itself by including the NAI along with the Mobile IP registration request.

Additionally, this feature allows you to configure the home agent to allocate addresses to mobile nodes either statically (including multiple static addresses per NAI flow) or dynamically. Home address allocation can be from address pools configured locally, through either DHCP server access, or from the AAA server.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftnaiadd.htm

Mobile IP Home Agent Policy Routing

The Mobile IP Home Agent Policy Routing feature supports route maps on Mobile IP tunnels created at the home agent. This feature allows an ISP to provide service to multiple customers. While reverse tunneling packets, the home agent looks up where the packet should go. For example, if an address corresponds to a configured network access identifier (NAI) realm name (such as cisco.com), the packet goes out interface 1, which has a connection to the Cisco network. If an address corresponds to another NAI realm name (such as nortel.com), the packet goes out interface 2, which has a connection to the Nortel network. This feature was designed to route traffics through VPNs back to an enterprise network.

Refer to the following document for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/fthapoli.htm

Mobile IP —IPsec for Home Agent to Foreign Agent Tunnel

The Mobile IP—IPsec for Home Agent to Foreign Agent Tunnel enables the use of IPSec on the home agent to foreign agent tunnel.

Crypto map configuration must be applied to both the tunnel and physical interfaces. For details refer to the “Configuring Cisco Encryption Technology” chapter in the Release 12.2 *Cisco IOS Security Configuration Guide*.

Mobile IP—MIB Support for NAI and HA Redundancy

The CISCO-MOBILE-IP-MIB is enhanced to add support for following features:

1. Compliance with RFC 2794 for mobile nodes identified by Network Access Identifiers (NAI).

The following tables are defined in the MIB to support NAI based mobile nodes (MN):

- cmiFaRegVisitorTable
- cmiHaRegCounterTable
- cmiSecAssocTable
- cmiSecViolationTable

These tables are the same as the corresponding tables in the RFC2006-MIB (MIP MIB) in terms of the information they provide, but indices are changed so that entries for mobile nodes which are not identified by the IP address will also be included in the table.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvpn13.htm

MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution

This feature enables you to configure your carrier supporting carrier network to enable Border Gateway Protocol (BGP) to transport routes and Multiprotocol Label Switching (MPLS) labels between the backbone carrier provider edge (PE) routers and the customer carrier customer edge (CE) routers. Previously you had to use Label Distribution Protocol (LDP) to carry the labels and an internal gateway protocol (IGP) to carry the routes between PE and CE routers to achieve the same goal.

This feature was originally introduced in Cisco IOS Release 12.0(21)ST. This release integrates the feature into Cisco IOS Release 12.2(13)T.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftcscl13.htm

MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

This feature enables you to set up a VPN service provider network so that the autonomous system boundary routers (ASBRs) exchange IPv4 routes with MPLS labels of the provider edge (PE) routers. Route reflectors (RRs) exchange VPNv4 routes, using multihop, multiprotocol, External Border Gateway Protocol (EBGP). This configuration saves the ASBRs from having to store all the VPNv4 routes. Using the route reflectors to store the VPNv4 routes and forward them to the PE routers results in improved scalability.

This feature was originally introduced in Cisco IOS Release 12.0(21)ST. This release integrates the feature into Cisco IOS Release 12.2(13)T.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftiasl13.htm

MPLS VPN-MIB Notifications

The MPLS VPN technology allows service providers to offer intranet and extranet VPN services that directly connect their customers' remote offices to a public network with the same security and service levels that a private network offers. The Provider-Provisioned VPN (PPVPN)-MPLS-VPN MIB notifications provide SNMP notification for critical MPLS VPN events.

The MPLS VPN-MIB Notifications feature provides the following benefits:

- A standards-based SNMP interface for retrieving information about critical MPLS VPN events.
- The generation and queuing of notifications that call attention to major changes in the operational status of MPLS VPN enabled interfaces; the forwarding of notification messages to a designated NMS for evaluation and action by network administrators.
- Advanced warning when VPN routing tables are approaching or exceed their capacity.
- Warnings about the reception of illegal labels on a VRF enabled interface. Such receptions may indicate misconfiguration or an attempt to violate security.

This feature was originally introduced in Cisco IOS Release 12.0(21)ST. This release integrates the feature into Cisco IOS Release 12.2(13)T.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvpnm13.htm

MS CHAP Version 2

The MS CHAP Version 2 feature in Cisco IOS Release 12.2(13)T introduces the ability of Cisco routers to utilize Microsoft Challenge Handshake Authentication Protocol Version 2 (MS CHAP V2) authentication for PPP connections between a computer using a Microsoft Windows operating system and a network access server (NAS). MS CHAP V2 authentication is an updated version of MS CHAP that is similar to, but incompatible with MS CHAP Version 1 (V1). MS CHAP V2 introduces mutual authentication between peers and a change password feature.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmschap.htm

Multicast-VPN—IP Multicast Support for MPLS VPNs

The Multicast-VPN—IP Multicast Support for MPLS VPNs feature allows a service provider to configure and support multicast traffic in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment. Because MPLS VPNs support only unicast traffic connectivity, deploying the Multicast-VPN feature in conjunction with MPLS VPN allows service providers to offer both unicast and multicast connectivity to MPLS VPN customers.

This feature supports routing and forwarding of multicast packets for each individual VPN routing and forwarding (VRF) instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone.

The Multicast-VPN feature in Cisco IOS software provides the ability to support the multicast feature over a Layer 3 VPN. As enterprises extend the reach of their multicast applications, service providers can accommodate these enterprises over their MPLS core network. IP multicast is used to stream video, voice, and data to an MPLS VPN network core.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmltvpn.htm

Multiclass Multilink PPP

Previous implementations of Cisco IOS Multilink PPP (MLP) include support for Link Fragmentatio Interleaving (LFI). This feature allows the delivery of delay-sensitive packets, such as the packets of a Voice call, to be expedited by omitting the PPP Multilink Protocol header and sending them as raw PPP packets in between the fragments of larger data packets. This feature works well on bundles consisting of a single link. However, when the bundle contains multiple links there is no way to keep the interleaved packets in sequence with respect to each other.

The Multiclass Multilink PPP (MCMP) feature in Cisco IOS Release 12.2(13)T addresses the limitations of MLP LFI on bundles containing multiple links by introducing multiple data classes. Normal data traffic and delay-sensitive data traffic are divided into Class 0 and Class 1, respectively. Class 0 data traffic is subject to fragmentation just as regular Multilink packets are. Class 1 data traffic can be interleaved but never fragmented. The next transmit sequence number, expected sequence number, unassigned fragment list, working packet, lost fragment timer, fastswitching mode, and all statistics are managed per-class, rather than for the bundle as a whole.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmmlppp.htm

NAT Default Inside Server

The NAT Default Inside Server feature provides for the need to forward packets from the outside to a specified inside local address. Traffic is redirected that does not match any Network Address Translation (NAT) entries and the packets are not dropped.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftnatis.htm

NAT Integration with MPLS VPNs

Network Address Translation (NAT) and MPLS VPNs can now be configured on a single device to work together. NAT can differentiate which MPLS VPN it receives IP traffic from even if the MPLS VPNs are all using the same IP addressing scheme. This enhancement enables MPLS VPN customers the ability to provide common shared services across multiple MPLS VPN customers while ensuring that each MPLS VPN is completely separate from the other.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftnatvpn.htm

NAT MIB (Read-Only)

This feature introduces support for the Network Address Translation (NAT) MIB. NAT provides tables for translating internal network addresses external network addresses. The NAT MIB provides objects for the monitoring and management of NAT bindings and session using SNMP. In this release, access to the MIB is limited to the read-only level. No new or modified Cisco IOS commands are associated with this MIB.

For details on the management options provided by the MIB, see the CISCO-IETF-NAT-MIB.my file available in the "SNMP v2 MIBs" section of the Cisco.com MIB page at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml. Additional information on the MIB is available in the form of an internet draft (draft-ietf-nat-natmib), available through www.ietf.org.

NAT Protocol Translation

Network Address Translation - Protocol Translation (NAT PT) is an IPv6 translation mechanism allowing IPv6-only devices to communicate with IPv4-only devices, and vice versa. NAT PT was designed using RFC 2766 as a migration tool to help customers transition their IPv4 networks to IPv6 networks. Using existing IPv4 NAT capability and adding a protocol translator allows NAT PT to provide direct communication between hosts speaking a different network protocol.

NAT Stateful Failover of Network Address Translation

There is an increasing need to provide highly resilient IP networks where application connectivity continues unaffected by potential failure to links and routers at the Network Address Translation (NAT) border. The Stateful NAT feature allows two or more network address translators to function as a translation group. A backup router running NAT provides translation services in the event of failure of the active translator.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftsnat.htm

NAT Support of H.323 RAS

Cisco IOS NAT supports all H.225 and H.245 message types, including those sent in the RAS protocol. RAS provides a number of messages that are used by software clients and Voice over IP (VoIP) devices to register their location, request assistance in call setup, and control bandwidth. The RAS messages are directed toward an H.323 gatekeeper.

Some RAS messages include IP addressing information in the payload, typically meant to register a user with the gatekeeper or learn about another user already registered. If these messages are not known to NAT, they cannot be translated to an IP address that will be visible to the public.

Previously, NAT did not support H.323 v2 RAS messages. With this enhancement, embedded IP addresses can be inspected for potential address translation.

This feature was previously released in Cisco IOS Release 12.2(4)T on the Catalyst 2900, Catalyst 2900XL, Catalyst 4000 series, Catalyst 5000 family switches with an installed Route Switch Module Catalyst 6000, Catalyst 8500 series, Cisco 800 series, Cisco 1000 series, Cisco1400 series, Cisco 16 series, Cisco 1700, Cisco 2600 series, Cisco 3600 series, Cisco 4000 series, Cisco 6400 series, Cisco 7000 series, Cisco 8500 series, Cisco 12000 series, Cisco MC3810, Cisco uBR900 series, Cisco uBR7200, and LightStream 1010 series platforms. This release is porting the feature into the IAD2420 platform.

NAT-Support of H.323 v2 Call Signaling

Cisco IOS NAT supports all H.225 and H.245 message types, including FastConnect and Alerting, as part of the H.323 v2 specification.

Previously, NAT only supported H.323 version 1 and that was specific only to the Microsoft NetMeeting application. With this enhancement, any product that makes use of these message types will be able to pass through a Cisco IOS NAT configuration without any static configuration.

This feature was previously released in Cisco IOS Release 12.1(5)T on the Cisco Catalyst 2900, Cisco Catalyst 2900XL, Cisco Catalyst 4000 series, Cisco Catalyst 5000 family switches with an installed Route Switch Module, Cisco Catalyst 6000 series, Cisco Catalyst 8500 series, Cisco LightStream 1010 series, Cisco 800 series, Cisco 1000 series, Cisco 1400 series, Cisco 1600 series, Cisco 1700 series, Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 4000 series, Cisco AS5300, Cisco AS5400, Cisco AS5800, Cisco 6400 series, Cisco 7000 series, Cisco 8500 series Cisco 12000 series, Cisco MC3810, Cisco uBR900, and Cisco uBR7200 platforms. This release is porting the feature into the Cisco IAD2420 platform.

NetWare Link Services Protocol (NLSP)

The NetWare Link Services Protocol (NLSP) will no longer be offered after Cisco IOS Release 12.2(13)T. NLSP commands will not appear in future releases of the Cisco IOS software documentation set.

Next Hop Resolution Protocol (NHRP) for IPX

The Next Hop Resolution Protocol (NHRP) for IPX will no longer be offered after Cisco IOS Release 12.2(13)T. NHRP for IPX commands will not appear in future releases of the Cisco IOS software documentation set.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

OSPF Support for Multi-VRF on CE Routers

The OSPF Support for Multi-VRF on CE Routers feature provides the capability of suppressing provider edge (PE) checks which are needed to prevent loops when the PE is performing a mutual redistribution of packets between the OSPF and BGP protocols. When VRF is used on a router that is not a PE (that is, one that is not running BGP), the checks can be turned off to allow for correct population of the VRF routing table with routes to IP prefixes.

OSPF multi-VRF allows you to split the router into multiple virtual routers, where each router contains its own set of interfaces, routing table, and forwarding table.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st21/ospfvrfl.htm

Packet Classification Based on Layer 3 Packet Length

This feature allows customers to match and classify traffic on the basis of the layer 3 length in the IP header of a packet. The layer 3 length is the IP datagram plus the IP header.

Traffic that matches a particular layer 3 length can be organized into specific classes that can, in turn, receive specific user-defined quality of service (QoS) treatment (for example, a certain amount of bandwidth or an IP Precedence value) when that class is included in a policy map.

This feature provides the added capability of matching and classifying traffic on the basis of the layer 3 length in the IP packet header. This new match criterion is in addition to the other match criteria, such as the IP precedence, differentiated services code point (DSCP) value, class of service (CoS), currently available.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmchpkt.htm

Packet Classification Using the Frame Relay DLCI Number

The Packet Classification Using the Frame Relay DLCI Number feature allows customers to match and classify traffic based on the Frame Relay data-link connection identifier (DLCI) number associated with a packet. This new match criterion is in addition to the other match criteria, such as the IP Precedence, Differentiated Service Code Point (DSCP) value, Class of Service (CoS), currently available.

The Packet Classification Using the Frame Relay DLCI Number feature extends the functionality of the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftpcdlci.htm

Per VRF AAA

Using the Per VRF AAA feature, Internet Service Providers (ISPs) can partition authentication, authorization, and accounting (AAA) services based on Virtual Route Forwarding (VRF). This feature permits the Virtual Home Gateway (VHG) to communicate directly with the customer's RADIUS server, which is associated with the customer's Virtual Private Network (VPN), without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer need to proxy AAA to provide their customers with the flexibility they demand.

This feature was originally introduced in Cisco IOS Release 12.2(1)DX. This release is porting the feature into the Cisco 7100 series, Cisco 7500 series, and Cisco 7700 series platforms.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvrfaaa.htm

Percentage-Based Policing and Shaping

This feature provides the ability to configure traffic policing and traffic shaping based on a *percentage* of bandwidth available on the interface. Configuring traffic policing and traffic shaping in this manner enables customers to use the same policy map for multiple interfaces with differing amounts of bandwidth.

PPPoE Client DDR Idle-Timer

This feature supports the dial-on-demand routing (DDR) interesting traffic control list functionality of the dialer interface with a PPP over Ethernet (PPPoE) client, but also keeps original functionality (PPPoE connection up and always on after configuration) for those PPPoE clients that require it.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftppecls.htm

Privilege Command Enhancement

This feature simplifies the configuration of privilege levels for specific commands through the enhancement of the **privilege level** global configuration command. A privilege level can now be specified for all keyword options of a command with a single command-line interface (CLI) command. Previously, separate "privilege level" commands were required for each keyword combination of a command. This enhancement can significantly reduce the number of commands needed to configure user privilege levels and correspondingly reduce the size of configuration files.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftprienh.htm

RADIUS Attribute 52 and Attribute 53 Gigaword Support

The RADIUS Attribute 52 and Attribute 53 Gigaword Support feature introduces support for Attribute 52 (Acct-Input-Gigawords) and Attribute 53 (Acct-Output-Gigawords) in accordance with RFC 2869. Attribute 52 keeps track of the number of times the Acct-Input-Octets counter has rolled over the 32-bit integer throughout the course of the provided service; attribute 53 keeps track of the number of times the Acct-Output-Octets counter has rolled over the 32-bit integer throughout the delivery of service. Both attributes can be present only in Accounting-Request records where the Acct-Status-Type is set to "Stop" or "Interim-Update." These attributes can be used to keep accurate track of and bill for usage.

This feature was originally introduced in Cisco IOS Release 12.2(4)B. No additional platform support has been added.

RADIUS Attribute 77 for DSL

The RADIUS Attribute 77 for DSL feature introduces support for Attribute 77 (Connect-Info) to carry the textual name of the virtual circuit class associated with the given permanent virtual circuit (PVC). (Although attribute 77 does not carry the unspecified bit rate (UBR), the UBR can be inferred from the classname used if one UBR is set up on each class.) Attribute 77 is sent from the network access server (NAS) to the RADIUS server via Accounting-Request and Accounting-Response packets.

This feature was originally introduced in Cisco IOS Release 12.2(4)B. No additional platform support has been added.

RADIUS Centralized Filter Management

Before the RADIUS Centralized Filter Management feature, wholesale providers (who provide premium charges for customer services such as access control lists [ACLs]) were unable to prevent customers from applying exhaustive ACLs, which could impact router performance and other customers. This feature introduces a centralized administration point—a filter server—for ACL management. The filter server acts as a centralized RADIUS repository for ACL configuration.

Whether or not the RADIUS server that is used as the filter server is the same server that is used for access authentication, the network access server (NAS) will initiate a second access-request to the filter server. If configured, the NAS will use the filter-id name as the authentication username and the filter server password for the second access-request. The RADIUS server will attempt to authenticate the filter-id name, returning any required filtering configuration in the access-accept.

Because downloading ACLs is time consuming, a local cache is maintained on the NAS. If an ACL name exists on the local cache, that configuration will be used without consulting the filter server.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_ftrmn.htm

RADIUS EAP Support

The EAP RADIUS Support feature allows users to apply to the client authentication methods that may not be supported by the network access server; this is done via the Extensible Authentication Protocol (EAP). Before this feature was introduced, support for various authentication methods for PPP connections required custom vendor-specific work and changes to the client and NAS.

EAP is an authentication protocol for PPP that supports multiple authentication mechanisms that are negotiated during the authentication phase (instead of the link control protocol [LCP] phase). EAP allows a third-party authentication server to interact with a PPP implementation through a generic interface.

This feature was originally introduced in Cisco IOS Release 12.2(2)XB5. This release is porting the feature into the Catalyst 4000, Cisco AS5350, Cisco AS5800, Cisco AS5850, Cisco 05, Cisco 806, Cisco 820, Cisco 1400 series, Cisco 1600 series, Cisco 1600R, Cisco 2500 series, Cisco 2600 series, Cisco 3620, Cisco 7100 series, Cisco 7200 series, Cisco 7500 series, Cisco MC3810, Cisco SOHO 70 series, Cisco SOHO78, Cisco uBR7200, Cisco uBR920

RADIUS Logical Line ID

The RADIUS Logical Line ID feature enables users to track their customers on the basis of the physical lines in which the customers' calls originate. Thus, users can better maintain the profile database of their customers as the customers move from one physical line to another.

Logical Line Identification (LLID) is an alphanumeric string (which must be a minimum of one character and a maximum of 253 characters) that is a logical identification of a subscriber line. LLID is maintained in a RADIUS server customer profile database. This customer profile database is connected to a L2TP access concentrator (LAC) and is separate from the RADIUS server that the LAC and L2TP Network Server (LNS) use for the authentication and authorization of incoming users. When the customer profile database receives a preauthorization request from the LAC, the server sends the LLID to the LAC as the Calling-Station-ID attribute (attribute 31).

The LAC sends a preauthorization request to the customer profile database when the LAC is configured for preauthorization. Configure the LAC for preauthorization using the subscriber access pppoe pre-authorize command.

This feature was originally introduced in Cisco IOS Release 12.2(8)B. No additional platform support has been added.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftlineid.htm

RSVP Local Policy Support

The RSVP Local Policy Support feature allows network administrators to create default and access control list (ACL)-based policies. These policies, in turn, control how RSVP filters its signalling messages to allow or deny quality of service (QoS) to networking applications based on the IP addresses of the requesting hosts.

This feature is being introduced in Cisco IOS Release 12.2(13)T.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftrsvplp.htm

RSVP Refresh Reduction and Reliable Messaging

The RSVP Refresh Reduction and Reliable Messaging feature includes refresh reduction, which improves the scalability, latency, and reliability of RSVP signalling by introducing the following extensions:

- Reliable messages (MESSAGE_ID, MESSAGE_ID_ACK objects, and ACK messages)
- Bundle messages (reception and processing only)
- Summary refresh messages (MESSAGE_ID_LIST and MESSAGE_ID_NACK objects)

This feature was originally introduced in Cisco IOS Release 12.2(11)S. This release integrates the feature into Cisco IOS Release 12.2(13)T.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftrsvpre.htm

Session Limit Per VRF

The Session Limit Per VPN Routing and Forwarding Instance (VRF) feature enables session limits to be applied on all VPDN groups associated with a common VPDN virtual template. Before the implementation of Session Limit Per VRF, a single default template carrying the configuration values of a subset of VPDN group commands were associated with all VPDN groups configured on the router. Session Limit Per VRF enables you to create, define and name multiple VPDN templates. You can then associate a specific template with a VPDN group. A session limit can be configured at the VPDN template level to specify a combined session limit for all VPDN groups associated with the configured VPDN template.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/12b_vrf.htm

Show Command Output Redirection

This feature adds the capability to redirect output from Cisco IOS CLI **show** commands to a file. For each show command issued, a new file can be created, or the output can be appended to an existing file. Command output can optionally be displayed on-screen while being redirected to a file by using the **tee** keyword. Redirection is available using a pipe (|) character after any **show** command, combined with the **redirect**, **append**, or **tee** keywords.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftshowre.htm

Simple Multicast Routing Protocol (SMRP) for AppleTalk

The Simple Multicast Routing Protocol (SMRP) for AppleTalk will no longer be offered after Cisco IOS Release 12.2(13)T. NLSP commands will not appear in future releases of the Cisco IOS software documentation set.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

SIP and H.323 Fax Enhancements

The SIP and H.323 Fax Enhancements feature adds an assortment of fax transfer enhancements to the Cisco IOS gateway implementations of H.323 and Session Initiation Protocol (SIP) call control protocols. The enhanced areas include the use of:

- H.323 and SIP fax pass-through
- H.323 and SIP T.38 fax relay fallback protocols
- H.323 and SIP NSE s for T.38 fax relay
- H.323 and SIP resource reservation (RSVP) protocol
- H.323 and SIP call admission control (CAC)

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftsihfax.htm

SIP—Call Transfer Enhancements Using the Refer Method

The SIP—Call Transfer Enhancements Using the Refer Method feature provides blind and attended call transfer capabilities to supplement the Bye and Also methods already implemented on Cisco IOS Session Initiation Protocol (SIP) gateways. The SIP—Call Transfer Enhancements Using the Refer Method feature is compatible with the original forms of call transfer and with third-party call-control protocols. The SIP—Call Transfer Enhancements Using the Refer Method feature enables application service providers (ASPs) to provide attended transfer and blind transfer in accordance with emerging SIP standards.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftsipref.htm

SIP Enhanced 180 Provisional Response Handling

This feature provides the ability to enable or disable early media cut-through on Cisco IOS gateways for SIP 180 response messages. The new feature allows you to specify whether 180 messages with Session Description Protocol (SDP) are handled in the same way as 183 responses with SDP. The 180 Ringing message is a provisional or informational response used to indicate that the INVITE message has been received by the user agent and that alerting is taking place. Both 180 and 183 messages may contain SDP which allow an early media session to be established prior to the call being answered.

Prior to the implementation of the new feature, Cisco gateways handled a 180 Ringing response with SDP in the same manner as a 183 Session Progress response; that is, the SDP was assumed to be an indication that the far end was going to send early media. Cisco gateways handled a 180 response without SDP by providing local ringback, rather than early media cut-through. The new feature provides the capability to ignore the presence or absence of SDP in 180 messages, and as a result, treat all 180 messages in a uniform manner.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft180sdp.htm

SIP Extensions for Caller Identity and Privacy

This feature provides support for privacy indication, as well as network verification and screening of a call participant's name and number. Cisco implements the new feature on Cisco SIP IOS trunking gateways by supporting a new header, Remote-Party-ID. In previous SIP implementations, the From header was used to indicate calling party identity, and once defined in the initial INVITE request, could not be modified for the duration of that session. Implementing the Remote-Party-ID header, which can be modified, added or removed as a call session is being established, overcomes previous limitations and enables call participant verification and screening

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftsipext.htm

SIP Gateway Compliance to RFC2543-bis-04

RFC2543-bis-04 contains several changes to Session Initiation Protocol (SIP) gateway code. The SIP Gateway Compliance to RFC2543-bis-04 feature updates Cisco SIP Voice over IP (VoIP) gateways with the latest RFC changes. All changes are compatible with older RFC versions. Some of the changes include:

- Comparison of SIP URLs for equality.

- 487 messages are now sent for BYE requests before disconnecting a call.
- Updated processing of 3xx redirection responses.
- Updated DNS SRV query procedures.
- Interpretation of user parameters before dial-peer matching.
- CANCEL requests can no longer have a route header.
- *user=phone* parameter no longer required in SIP URLs.
- Obsoletion of the 303 and 411 SIP cause codes.
- The Content-Type header can now have an empty Session Description Protocol (SDP) body.
- Optional "s=" line in Session Description Protocol (SDP).
- Inclusion of Allow headers to INVITEs and 2xx responses.
- Use of simultaneous Cancel and 2xx Class Responses.

SIP Redirect Processing Enhancements

The SIP Redirect Processing Enhancements feature allows flexibility in the handling of incoming redirect or 3*xx* class of responses so they can be enabled or disabled through the command-line interface (CLI). The default mode is enabled, in which Session Initiation Protocols (SIP) gateways handle incoming 3*xx* messages as per RFC 2543. RFC 2543 states that redirect response messages are used by SIP user agents (UA) to initiate a new Invite when a UA learns that a user has moved from a previously known location. If redirect handling is disabled through the CLI, the UA treats incoming 3*xx* responses as 4*xx* error class responses. The call is not redirected, and is instead released with the appropriate PSTN cause code.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftsipmaz.htm

SNMP Notification Logging

Systems that support Simple Network Management Protocol (SNMP) often need a mechanism for recording notification information as a hedge against lost notifications, whether those are traps or informs that exceed retransmission limits. The Notification Log MIB provides a common infrastructure for other MIBs in the form of a local logging function. The SNMP Notification Logging feature adds Cisco IOS command-line interface (CLI) commands to change the size of the notification log, to set the global ageout value for the log, and to display logging summaries at the command line.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/ftmiblog.htm

SSG Autologoff

The SSG Autologoff feature enables the Cisco Service Selection Gateway (SSG) to verify connectivity with each host at configured intervals. If SSG detects that the host is not reachable from SSG, then it automatically initiates the logoff for that host.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/index.htm

SSG Port-Bundle Host Key

The SSG Port-Bundle Host Key feature enhances communication and functionality between the Service Selection Gateway (SSG) and the Cisco Subscriber Edge Services Manager (SESM) by introducing a mechanism that uses the host source IP address and source port to identify and monitor subscribers.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/index.htm

SSG TCP Redirect for Services

The SSG TCP Redirect for Services feature redirects certain packets, which would otherwise be dropped, to captive portals that can handle the packets in a suitable manner. For example, packets sent upstream by unauthorized users are forwarded to a captive portal that can redirect the users to a logon page. Similarly, if users try to access a service to which they have not logged on, the packets are redirected to a captive portal that can provide a service logon screen.

The captive portal can be any server that is programmed to respond to the redirected packets. If the Cisco Subscriber Edge Services Manager (SESM) is used as a captive portal, unauthenticated subscribers can be sent automatically to the SESM logon page when they start a browser session. In SESM Release 3.1(3), captive portal applications can also redirect to service logon pages, advertising pages, and message pages. The SESM captive portal application can also capture a URL in a subscriber's request and redirect the browser to the originally requested URL after successful authentication. Redirected packets are always sent to a captive portal group that consists of one or more servers. SSG selects one server from the group in a round-robin fashion to receive the redirected packets.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ssg/index.htm

Subscriber Service Switch (SSS)

The Subscriber Service Switch (SSS) was developed in response to a need by Internet service providers for increased scalability and extensibility for remote access service selection and Layer 2 subscriber policy management. This Layer 2 subscriber policy is needed to manage tunneling of PPP, Ethernet, Frame Relay, and other link-level protocols in a policy-based bridging fashion

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_sss.htm

Support for IPsec ESP Through NAT

The ability to support multiple concurrent IPsec ESP tunnels or connections through a router configured with Network Address Translation (NAT) can now be utilized when the NAT router is configured in overload or Port Address Translation (PAT) mode.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftnatesp.htm

T.38 Fax Relay for VoIP H.323

T.38 Fax Relay for VoIP H.323 provides standards-based fax relay protocol support for H.323 gateways and gatekeepers. T.38 is an ITU-T recommended standard for fax relay. Since T.38 is a standards-based implementation for fax relay, Cisco gateways and gatekeepers are able to interwork with third-party H.323 devices that support T.38 protocol.

This feature was previously released in Cisco IOS Release 12.1(3)T on Cisco 2600 series, Cisco 3640, and Cisco MC3810 platforms. This release is porting the feature into the IAD2420 platform.

Terminal Line Security for PAD Connections

X.25 closed user group (CUG) service is a network service that allows subscribers to be segregated into private subnetworks with limited outgoing and incoming access. A data terminal equipment (DTE) device becomes a member of a CUG by subscription; the DTE must obtain membership from its network service for the set of CUGs to which it needs access.

The Terminal Line Security for PAD Connections feature allows CUG services to be configured on terminal lines, enabling terminal lines to participate in X.25 CUG security for packet assembler/disassembler (PAD) connections. CUG services can be applied to console lines, auxiliary lines, and tty and vty devices. Configuring CUG services on terminal lines allows you to specify CUG protection for lines that are part of the point of presence (POP). Before the introduction of this feature, CUG services could be configured only on X.25 synchronous data communications equipment (DCE) interfaces.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftcugpad.htm

Update to the Interworking of Cisco MGCP Voice Gateways and Cisco CallManager Version 3.2 Feature

This document describes updates to the *Interworking of Cisco MGCP Voice Gateways and Cisco Call Manager Version 3.2* feature. This update introduces the **mgcp validate domain-name** command, which enables you to check if the domain name or host name and the IP address received as part of the endpoint names sent from the Call Agent (CA) or Cisco CallManager (CCM) match with the ones that have been configured on the gateway (GW). This check is valid for the MGCP messages received from the CA or CCM only.

Use the new **mgcp validate domain-name** command first before configuring MGCP in a Voice over IP (VoIP) network.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvalid.fm

Update to the playout-delay Command

In environments with long network delays, T.38 fax relay can be unsuccessful. The **fax** keyword was added to the **playout-delay** command to allow users to decrease the playout delay value to compensate for long network delays when necessary.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ft_pdfax.htm

Virtual Router Redundancy Protocol (VRRP)

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

- Proxy ARP—The client uses Address Resolution Protocol (ARP) to get the destination it wants to reach, and a router will respond to the ARP request with its own MAC address.
- Routing protocol—The client listens to dynamic routing protocol updates (for example, from Routing Information Protocol [RIP]) and forms its own routing table.
- IRDP (ICMP Router Discovery Protocol) client—The client runs an Internet Control Message Protocol (ICMP) router discovery client.

The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segme and is cut off from the rest of the network.

The Virtual Router Redundancy Protocol (VRRP) feature can solve the static configuration problem. VRRP enables a group of routers to form a single *virtual router*. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

VRRP is supported on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, and on MPLS VPNs and VLANs.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st18/st _vrrpx.htm

VLAN Range

Using the VLAN Range feature, you can group VLAN subinterfaces together so that any command entered in a group applies to every subinterface within the group. This capability simplifies configurations and reduces command parsing.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/1. b_rang.htm

Voice and Quality of Service Features for ADSL and G.SHDSL on Cisco 1700, Cisco 2600, and Cisco 3600 Series Routers

Cisco 1700 series, Cisco 2600 series, and Cisco 3600 series routers with ADSL or G.SHDSL WAN interface cards support the integration of voice and data over the same ADSL or G.SHDSL circuit using Voice over IP (VoIP). Cisco 2600 series and Cisco 3600 series routers with ADSL or G.SHDSL WAN interface cards also support the integration of voice and data over the same ADSL or G.SHDSL circuit using Voice over ATM (VoATM).

This feature was originally introduced in Cisco IOS Release 12.2(4)XL. This release is porting the feature into the Cisco 1700 series platforms.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xl/122x14/ft_qgdsl.htm

Voice Call Tuning

This feature provides tools for quickly taking spot performance measurements of voice call performance while the call is up. You also have the ability to change the echo canceller and jitter buffer parameters of a call while the call is in progress. Audible effects can be immediately noticed, aiding in problem determination and resolution. The feature provides real-time call monitor and manipulation on the interface between Cisco IOS software and the digital signalling processors (DSPs) by addressing the following two items:

- Development of real-time status of a call, including packet flow indication, DSP state, echo canceller state, and jitter state.
- Real-time manipulation of echo canceller and jitter buffer parameters.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftvdsptn.htm

VPDN Multihop by DNIS

The Cisco VPDN Multihop by DNIS feature allows dialed number identification service (DNIS)-based multihop capability in a virtual private dial-up network (VPDN), which enables customers that dial in to a network using a standard telephone line to take advantage of the aggregation capability offered by multihop switching.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_8/ftvmhopd.htm

VRRP Support

There are several ways a LAN client can determine which router should be the first hop to a particular remote destination. The client can use a dynamic process or static configuration. Examples of dynamic router discovery are as follows:

- Proxy ARP
- Routing protocol
- IRDP (ICMP Router Discovery Protocol) client

The drawback to dynamic discovery protocols is that they incur some configuration and processing overhead on the LAN client. Also, in the event of a router failure, the process of switching to another router can be slow.

An alternative to dynamic discovery protocols is to statically configure a default router on the client. This approach simplifies client configuration and processing, but creates a single point of failure. If the default gateway fails, the LAN client is limited to communicating only on the local IP network segment and is cut off from the rest of the network.

The Virtual Router Redundancy Protocol (VRRP) feature can solve the static configuration problem. VRRP enables a group of routers to form a single *virtual router*. The LAN clients can then be configured with the virtual router as their default gateway. The virtual router, representing a group of routers, is also known as a VRRP group.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st18/st_vrrpx.htm

X.25 Suppression of Security Signaling Facilities

This feature allows the X.25 Call Redirection/Call Deflection Notification (CRCDN) and Called Line Address Modified Notification (CLAMN) security signaling facilities to be disabled (suppressed) in packets that transit data communication equipment that uses a mix of International Telecommunication Union Telecommunication Standardization Sector T (ITU-T) 1980 and 1984 X.25 protocols.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftsupsgx.htm

Xerox Network Systems (XNS)

The Xerox Network Systems (XNS) feature will no longer be offered after Cisco IOS Release 12.2(13)T. XNS commands will not appear in future releases of the Cisco IOS software documentation set.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftjencrg.htm

New Hardware Features Supported in Cisco IOS Release 12.2(11)T1

The following new hardware features are supported in Cisco IOS Release 12.2(11)T1. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

Cisco 3640A Router

The Cisco 3640A is identical to the Cisco 3640 router in terms of physical characteristics, interface support, performance and memory. The Cisco 3640A router will support the same Cisco IOS feature sets as the Cisco 3640 router, but requires a different minimum version of Cisco IOS software.

Hardware Platforms and Modules Newly Supported in Cisco IOS Release 12.2(11)T

The following hardware platforms and modules are now supported in Cisco IOS Release 12.2(11)T. These platforms and modules were first introduced in earlier Cisco IOS software releases.

16-Port Ethernet Switch Module for Cisco 2600 Series and Cisco 3600 Series

The 16-port Ethernet switch network module was originally introduced in Cisco IOS Release 12.2(8)T. Cisco IOS Release 12.2(11)T adds stacking and flow control features to the previously released feature.

See the “16-Port Ethernet Switch Module for Cisco 2600 Series and Cisco 3600 Series” section on page 224 or refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft1636nm.htm.

Cisco 1760 Router

The Cisco 1760 router is a voice-and-data-capable router that provides Voice-over-IP (VoIP) functionality and can carry voice traffic (for example, telephone calls and faxes) over an IP network. Using one or two WAN connections, the router links small-to-medium-size remote Ethernet and Fast Ethernet LANs to central offices.

The Cisco 1760 router is available in two models. The Cisco 1760 runs data and data-plus-voice images, providing digital and analog voice support. The Cisco 1760-V includes all the features needed for immediate integration of data and voice services with support for multiple voice channels.

Refer to the documents at the following location for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/index.htm.

Cisco AS5350 Universal Gateway

The Cisco AS5350 Universal Gateway is the only one-rack-unit, two, four, or eight PRI gateway that provides universal services—data, voice, and fax services on any service, any port. The Cisco AS5350 offers high performance and high reliability in a compact, modular design. This cost-effective platform is ideally suited for Internet service providers (ISPs) and enterprises that require innovative universal services.

Refer to the documents at the following location for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5350/index.htm.

Cisco AS5850 Universal Gateway

The Cisco AS5850 Universal Gateway provides the highest concentration of port and Integrated Services Digital Network (ISDN) terminations available in a single remote access server product. The Cisco AS5850 is specifically designed to meet the demands of large service providers such as Post, Telephone, and Telegraphs (PTTs), regional bell operating companies (RBOCs), inter-exchange carriers (IXCs), and large Internet service providers (ISPs).

Refer to the documents at the following location for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5850/index.htm.

Cisco Signaling Link Terminal (SLT) Dual Ethernet

The Cisco Signaling Link Terminal (SLT) Dual Ethernet feature adds Cisco Cisco Signaling Link Terminal dual Ethernet support to the virtual switch controller (VSC). This enhanced Cisco SLT support provides two IP networks and two additional Session Manager sessions (for a total of four Session Manager sessions) for improved backhaul communication. These additions increase the resilience of Cisco SLT and VSC communications by supporting two Reliable User Datagram Protocol (RUDP) sessions from each Ethernet interface to each VSC. These VSC enhancements help to determine when to switch Ethernets and when to switch VSC activity.

The Cisco SLT, which is based on the Cisco 2611 router, is shipped with two Ethernet interfaces. Until this feature was released, the Cisco SLT and VSC solution supported only one of the two Ethernet interfaces. Both Session Manager sessions had to travel over this single Ethernet interface. The Cisco Signaling Link Terminal Dual Ethernet feature supports the second Ethernet, which improves the resilience of the backhaul IP communications.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftsltdua.htm.

New Software Features in Cisco IOS Release 12.2(11)T

The following new features are supported in Cisco IOS Release 12.2(11)T. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

AAA-PPP-VPDN Non-Blocking

Previously, Cisco IOS created a statically configurable number of processes to authenticate calls. Each of these processes would handle a single call, but in some situations the limited number of processes could not keep up with the incoming call rate. This resulted in some calls timing out. The AAA-PPP-VPDN Non-Blocking feature changes the software architecture such that the number of processes will not limit the rate of call handling.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Accounting of VPDN Disconnect Cause

In the past, whenever a Layer 2 Tunneling Protocol (L2TP) or Layer 2 Forwarding (L2F) session fails or disconnects, the network access server (NAS) and Home GateWay (HGW) report a very generic disconnect-cause code, such as "LOST CARRIER". These generic codes do not provide enough detailed information for accounting and debugging purposes, creating a need for disconnect-cause codes that provide more detailed information. The Accounting of VPDN Disconnect Cause feature adds eight new disconnect-cause codes. These eight disconnect-cause codes describe the status of Virtual Private Dialup Network (VPDN) failures and disconnects more specifically than existing generic disconnect-cause codes. These new disconnect-cause codes can be found in the *Cisco IOS Security Configuration Guide*, Release 12.2 located at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fappendx/fradattr/scfrdat3.htm.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftacldir.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

ACL Authentication of Incoming rsh and rcp Requests

To enable the Cisco IOS software to receive incoming remote shell (rsh) protocol and remote copy (rcp) protocol requests, customers must configure an authentication database to control access to the router. This configuration is accomplished by using the **ip rcmd remote-host** command.

Currently, when using this command, customers must specify the local user, the remote host, and the remote user in the database authentication configuration. For users who can execute commands to the router from multiple hosts, multiple database authentication configuration entries must be used, one for each host.

This feature allows customers to specify an access list for a given user. The access list identifies the hosts to which the user has access. A new argument, *access-list*, has been added that can be used with this command to specify the access list.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftauth.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

ACL Default Direction

The ACL Default Direction feature allows you to change the filter direction (where filter direction is not specified) to inbound packets only; that is, you can configure your server to filter packets that are coming toward the network.

This feature introduces the **radius-server attribute 11 direction default** command, which allows you to change the default direction of filters for your access control lists (ACL) via RADIUS. (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user.) Enabling this command allows you to change the filter direction to inbound—which stops traffic from entering a router, thereby reducing resource consumption—rather than the outbound default direction, which waits until the traffic is about to leave the network before filtering. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftacldir.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Advanced Voice Busyout

The local voice busyout feature provides a way to busy out a voice port or DS-0 group (time slot) if a state change is detected in a monitored network interface (or interfaces). When a monitored interface changes to a specified state—to out-of-service or in-service—the voice port presents a seized/busyout condition to the attached PBX or other customer premises equipment (CPE). The PBX or other CPE can then attempt to select an alternate route.

Advanced Voice Busyout adds the following functionality to the local voice busyout feature:

- For Voice over IP (VoIP), monitoring of links to remote, IP-addressable interfaces by use of service assurance agent (SAA)
- Configuration by voice class to simplify and speed up the configuration of voice busyout on multiple voice ports

Using the Advanced Voice Busyout feature you can perform the following tasks:

- Configure individual voice ports to enter the busyout state if an SAA probe signal returned from a remote, IP-addressable interface detects loss of IP connectivity by crossing a specified delay or loss threshold.
- Define voice classes with specified busyout conditions, and assign a particular voice class to any number of voice ports.
- SAA probe monitoring of remote interfaces is intended for use with VoIP networks, although it can also be used with Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_cacbo.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(3)T. Cisco IOS Release 12.2(4)T ported the feature into the Cisco 7200 series routers and added support for new and modified commands. This release is porting the feature into the 1760 routers and the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Analog Centralized Automatic Message Accounting E911 Trunk

Cisco IOS Release 12.2(11)T is the first Cisco IOS release that introduces the Analog Centralized Automatic Message Accounting (CAMA) E911 feature that adds E911 connectivity features to the Cisco 2600 series and Cisco 3600 series routers.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/acam_911.htm.

Asynchronous Line Monitoring

Before Cisco IOS Release 12.2(4)T, the Cisco IOS software did not provide a method for displaying asynchronous character mode traffic flowing out of an asynchronous line. Therefore, when a user tried to troubleshoot difficult asynchronous problems, the user had to use RS-232 datascopes to examine the data stream. This method is detailed and cumbersome. The Asynchronous Line Monitoring feature that is available in Cisco IOS Release 12.2(4)T allows the monitoring of inbound and outbound character mode asynchronous traffic on another terminal line. To monitor inbound or outbound asynchronous character mode traffic on the port to be monitored, enter the **monitor traffic line** command in privileged EXEC mode.

This feature increases the efficiency of the user who performs troubleshooting on asynchronous character mode traffic problems.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftasync.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

ATM Service Level Monitoring (SLM)

The Cisco Service Assurance Agent (SA Agent) is an embedded performance monitoring utility in Cisco IOS software. The ATM Service Level Monitoring (SLM) feature expands the capabilities of the SA Agent to provide detailed monitoring statistics for your ATM network. Monitoring service levels for ATM connections allows service providers to ensure that their networks are meeting or exceeding the performance outlined in service level agreements (SLAs).

The ATM Service Level Monitoring feature can also be used with Cisco Networking Services (CNS). A device running CNS, such as the IE2100, can be used to retrieve the ATM performance statistics generated by the SA Agent. Additionally, these results can be passed to other devices running third-party monitoring software.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftatmslm.htm

Barge-In and Busy Line Verify Operator Services

The Barge-In and Busy Line Verify Operator Services feature enhances Simple Gateway Control Protocol (SGCP)/Media Gateway Control Protocol (MGCP) gateway conferencing capabilities to support the Busy Line Verification/Operator Interrupt (BLV/OI) feature. The Busy Line Verification feature permits an operator to establish a connection to a customer's line to verify a busy condition for a calling party. The Operator Interrupt feature allows the operator to speak to the customer and to connect the calling party and customer, if appropriate. These enhancements support other call flows such as call pickup with barge-in that require the ability to conference a second call into an existing two-party call without intervention by parties in the existing call. No explicit configuration is required to enable this feature.

The MGCP Basic CLASS and Operator Services feature introduced conferencing to support three-way calling on SGCP and MGCP gateways. It is described in MGCP Basic CLASS and Operator Services at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcpgr.htm.

Basic Service Relationships (H.225 Annex G)

Cisco's H.225 Annex G implements the minimal set of Annex G features needed to allow Cisco border elements to interoperate with any ClearingHouse border element. This feature enhances Cisco's H.225.0 Annex G support to include basic Service Relationships and Usage Reporting. The feature provides enhanced interoperability with a ClearingHouse border element and third party border element as well as address resolution for interdomain call routing.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_srang.htm.

BGP Conditional Route Injection

Cisco IOS software provides several methods in which you can originate a prefix into the Border Gateway Protocol (BGP). The existing methods include using the network or **aggregate-address** commands and redistribution. These methods assume the existence of more specific routing information (matching the route to be originated) in either the routing table or the BGP table.

The BGP Conditional Route Injection feature enables you to originate a prefix into BGP without the corresponding match. The routes are injected into the BGP table only if certain conditions are met. The most common condition is the existence of a less-specific prefix.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11bpri.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

BGP Hide Local-Autonomous System

The BGP Hide Local-Autonomous System feature introduces the **no-prepend** keyword to the **neighbor local-as** command. The use of the **no-prepend** keyword allows a network operator to configure a Border Gateway Protocol (BGP) speaker to not prepend the local autonomous system number to any routes that are received from external peers. This feature can be used to help transparently change the autonomous system number of a BGP network and ensure that routes can be propagated throughout the autonomous system, while the autonomous system number transition is incomplete. Because the local autonomous is not prepended to these routes, external routes will not be rejected by internal peers during the transition from one autonomous system number to another.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11bhla.htm
.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

BGP Link Bandwidth

The Border Gateway Protocol (BGP) Link Bandwidth feature is used to advertise the bandwidth of an autonomous system exit link as an extended community. The BGP Link Bandwidth feature is supported by the internal BGP (iBGP) and external BGP (eBGP) multipath features. The link bandwidth extended community indicates the preference of an autonomous system exit link in terms of bandwidth. The link bandwidth extended community attribute may be propagated to all iBGP peers and used with the BGP multipath features to configure unequal cost load balancing. When a router receives a route from a directly connected external neighbor and advertises this route to iBGP neighbors, the router may advertise the bandwidth of that link. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11b_lb.htm
.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco 5800 platforms.

BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN

The BGP Multipath Load Sharing for eBGP and iBGP feature allows you to configure multipath load balancing with both external BGP (eBGP) and internal BGP (iBGP) paths in Border Gateway Protocol (BGP) networks that are configured to use Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). This feature provides improved load balancing deployment and service offering capabilities and is useful for multi-homed autonomous systems and Provider Edge (PE) routers that import both eBGP and iBGP paths from multihomed and stub networks. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11bmpl.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

BGP Prefix-Based Outbound Route Filtering

The BGP Prefix-Based Outbound Route Filtering feature uses Border Gateway Protocol (BGP) outbound route filter (ORF) send and receive capabilities to minimize the number of BGP updates that are sent between peer routers. The configuration of this feature can help reduce the amount of resources required for generating and processing routing updates by filtering out unwanted routing updates at the source. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11borf.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Call Admission Control Based on CPU Utilization

The Preauthentication with ISDN PRI feature permits the Cisco AS5300 and AS5800 universal access servers to deny incoming calls exceeding a preconfigured threshold, permitting the selection of a system CPU load level value. This feature helps ensure the quality of service (QoS) of existing calls and reliability of system processes by preventing system overload that is caused by excessive incoming calls. The feature rejects new digital calls (PRI, channel-associated signaling [CAS], and ISDN), with minor disruption to system users.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/ios_122/dt61294.htm.

Call Admission Control for H.323 VoIP Gateways

Before the call admission control feature was available, gateways did not have a mechanism to prevent calls from entering when certain resources were not available to process the call. This situation caused new calls to fail with unreported behavior and potentially caused the calls in progress to have quality-related problems.

This feature set provides the ability to support resource-based call admission control processes. These resources include system resources such as CPU, memory, and call volume and interface resources such as call volume.

If system resources are not available to admit the call, the following two kinds of actions are provided: system denial (which busy outs all of T1 or E1) or per-call denial (which disconnects, hairpins, or plays a message or tone). If the interface-based resource is not available to admit the call, the call is dropped from the session protocol (such as H.323).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftcac58.htm.

Note The Call Admission Control for H.323 VoIP Gateways feature was previously released in Cisco IOS Release 12.2(4)T on the Cisco 2600 and Cisco 3600 routers and Cisco MC3810 multiservice concentrators. This feature has been added to the Cisco AS5300, Cisco AS5800, and Cisco AS5850 in Cisco IOS Release 12.2(11)T.

Call Status Tracking Optimization

In an H.323 Voice-over-IP (VoIP) network, gatekeepers use information request (IRQ) messages to obtain information about a certain call or all calls from an endpoint (for example, an originating gateway). The gatekeeper can send an IRQ to request information from the endpoint, which responds with an information request response (IRR). The gatekeeper can also use the IRR Frequency field in the initial admission confirm (ACF) message to instruct the endpoint to periodically report with IRR messages during call admission.

Currently, the Cisco gatekeeper maintains the call states of all calls it has admitted to track bandwidth usage. In addition, the gatekeeper must be able to reconstruct call structures for a newly transferred gateway from an alternate gatekeeper, if a gatekeeper switchover has occurred. In a gatekeeper switchover, the new gatekeeper sends an IRQ message with the call reference value (CRV) set to zero to the newly registered gateway to obtain information about existing calls before the switchover.

If a gateway supports a large volume of calls, the number of IRR messages as responses to an IRQ with the CRV set to zero could be CPU intensive and cause congestion. Additionally, if a gatekeeper serves many endpoints or high-capacity gateways, the IRQ requests and the resulting IRR messages received can flood the network, causing high CPU utilization and network congestion.

The Call Status Tracking Optimization feature provides the following methods to address this potential problem:

- A command-line interface (CLI) command to configure IRR frequency that is included in the ACF message. Currently, the IRR frequency is set to 240 seconds (4 minutes), based on an average 4-minute call hold time. The IRR allows the gatekeepers to terminate calls for which a disengage request (DRQ) has not been received. If missing DRQs are not a problem, the IRR frequency can be set to a larger value than 4 minutes, minimizing the number of unnecessary IRRs sent by a gateway.

- A CLI command to disable the gatekeeper from sending an IRQ with the CRV set to zero when the gatekeeper is requesting the status of all calls after its initialization. Disabling the IRQ can eliminate unnecessary IRR messages in cases where the reconstruction of call structures can be postponed until the next IRR, or in cases where the call information is no longer required because calls are terminated before the periodic IRR is sent. Disabling the IRQ is advantageous if direct bandwidth control is not used in the gatekeeper.
- The number of retries for sending the DRQ is increased from two to nine. If the reliability of DRQ messages is increased, a longer period can be used before the next IRR is sent. Increasing the number of DRQ retries from two to nine increases DRQ reliability. This value is not configurable.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_csto2.htm.

Call Tracker show Commands Extensions

Before Cisco IOS Release 12.2(11)T, the **show calltracker active** EXEC command and the **show calltracker history** EXEC command provided a simple way to examine the Call Tracker active table and Call Tracker history table in chronological order. The extensions to these commands available in Cisco IOS Release 12.2(11)T allow the command output to be reverse collated (output from most recent to least recent) or to be filtered by call category or service type. Historical data for disconnected call sessions can be filtered by subsystem type.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftcall.htm.

CEF on Multipoint GRE Tunnels

The CEF on Multipoint GRE Tunnels feature enables Cisco Express Forwarding (CEF) switching of IP traffic to and from multipoint generic routing encapsulation (GRE) tunnels. Tunnel traffic can be forwarded to a prefix through a tunnel destination when both the prefix and the tunnel destination are specified by the application.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T as CEF-Switched Multipoint GRE Tunnel. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Certificate Autoenrollment

The Certificate Autoenrollment feature allows you to configure your router to automatically request a certificate from the certification authority (CA) that is using the parameters in the configuration. Thus, operator convention is no longer required at the time the enrollment request is sent to the CA server.

Automatic enrollment will be performed on startup for any trustpoint CA that is configured and does not have a valid certificate. When the certificate—which is issued by a trustpoint CA that has been configured for autoenrollment—expires, a new certificate is requested. Although this feature does not provide seamless certificate renewal, it does provide unattended recovery from expiration.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftautoen.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 platforms.

Certificate Enrollment Enhancements

The Certificate Enrollment Enhancements feature introduces five new subcommands to the **crypto ca trustpoint** command—**ip-address** (ca-trustpoint), **password** (ca-trustpoint), **serial-number**, **subject-name**, and **usage**. These commands provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts. (However, the prompting behavior remains the default if this feature is not enabled.) Thus, users can preload all necessary information into the configuration, allowing each router to obtain its certificate automatically when it is booted.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftenrol2.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 platforms.

Circuit Interface Identification Persistence for SNMP

The Circuit Interface MIB (CISCO-CIRCUIT-INTERFACE-MIB) provides a MIB object (cciDescr) which can be used to identify individual circuit-based interfaces for SNMP monitoring. The Circuit Interface Identification Persistence for SNMP feature maintains this user-defined name of the circuit across reboots, allowing the consistent identification of circuit interfaces. Circuit Interface Identification Persistence is enabled using the **snmp mib persist circuit** global configuration command.

Note This feature was originally introduced in Cisco IOS Release 12.1(4)T. This release is porting the feature into the Cisco AS5300 platform.

Cisco Gateway Management Agent

The Cisco Gateway Management Agent (CGMA) feature provides an eXtensible Markup Language (XML) interface to support real-time management of a Cisco IOS gateway (GW). Currently, GWs provide statistics using Simple Network Management Protocol (SNMP) and do not support real-time polling. The CGMA feature allows GWs to communicate with third-party management applications using XML over TCP/IP.

Note The Cisco Gateway Management Agent feature was previously released in Cisco IOS Release 12.2(8)T on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 7200 series routers. In Cisco IOS Release 12.2(11)T, this feature is now supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Cisco Gateway Management Agent (CGMA) Phase 2

The Cisco Gateway Management Agent (CGMA) Phase 2 feature provides additional enhancements for the Cisco Gateway Management Agent (CGMA) feature. The CGMA provides an eXtensible Markup Language (XML) interface to support real-time management of a Cisco IOS gateway. Currently, gateways provide statistics using Simple Network Management Protocol (SNMP) and do not support real-time polling. The CGMA feature allows gateways to communicate with third-party management applications using XML over TCP/IP.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftcgma2.htm.

Note The Cisco Gateway Management Agent (CGMA) Phase 2 feature was previously released in Cisco IOS Release 12.2(8)T on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 7200 series routers. In Cisco IOS Release 12.2(11)T, this feature is now supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Cisco H.323 Multizone Enhancements

The Cisco H.323 Multizone Enhancements feature enables the Cisco gateway to provide information to the gatekeeper with the use of additional fields in the RAS (registration, admission, and status) messages.

Previously, the source gateway attempted to set up a call to a destination IP address as provided by the gatekeeper in an Admission Confirm (ACF) message. If the gatekeeper was unable to resolve the destination E.164 phone number to an IP address, the incoming call was terminated.

This version of the H.323 software adds support to allow a gatekeeper to provide additional destination information and modify the destinationInfo field in the ACF. The gateway will include the canMapAlias associated destination information in setting up the call to the destination gateway.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/ios_122/pul0244x.htm.

Note This feature was originally introduced in Cisco IOS Release 12.0(7)T on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 7200 series routers, and the Cisco MC3810 and Cisco AS5300 platforms. This release is porting the feature into the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Cisco IOS Telephony Service Version 2.0

The Cisco IOS Telephony Service Version 2.0 feature was previously released in Cisco IOS Release 12.2(8)T. In Cisco IOS Release 12.2(11)T, there are minor enhancements to this feature, which is now referred to as Cisco IOS Telephony Service Version 2.01. Refer to the following document for information about the enhancements added to this release:

http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/ipkey2.htm.

Cisco VCWare Version Checker

The Cisco VCWare Version Checker feature adds Cisco VCWare version checker warning output at bootup and when you use the **show vfc version vcware** and **show vfc version dspware** commands.

This new version checker feature detects possible mismatches between Cisco IOS software and Cisco VCWare and DSPWare. If a software mismatch is found, a compatibility mismatch warning is output at bootup and when the **show vfc version** commands are used. If no mismatch is found, there is no advisory output. Because the new information is advisory only, there is no action taken whether the software is compatible or incompatible.

This feature applies only to the Cisco AS5300. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftvdspck.htm

CISCO-BULK-FILE-MIB Enhancements

The Cisco Bulk File Creation MIB (CISCO-BULK-FILE-MIB.my) is a MIB module for creating and deleting bulk files of SNMP data for file transfer. The CISCO-BULK-FILE-MIB Enhancements featu enhances the Cisco Bulk File Creation MIB to support selective-row-transfer and notification-on-file-creation. Prior to this enhancement, when the MIB was used to dump large tables (for example, the ccHistoryTable), much of the data transfer consisted of duplicated data. This feature allows the SNMP manager to specify a starting row in the SNMP Get request.

This feature also introduces a notification that can be sent when file creation is complete or when there is an error during file creation. Specifically, this feature modifies the CISCO-BULK-FILE-MIB by introducing four new MIB objects (cbfDefineFileNotifyOnCompletion, cbfDefineObjectTableInstance, cbfDefineObjectNumEntries, cbfDefineObjectLastPolledInst) and a new notification object (cbfDefineFileCompletion). For details, refer to the CISCO-BULK-FILE-MIB.my file, available through Cisco.com MIB FTP site at the following URL:

ftp://ftp.cisco.com/pub/mibs/v2/CISCO-BULK-FILE-MIB.my.

Note This feature was originally introduced in Cisco IOS Release 12.1(8)T. This release is porting the feature into the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

CISCO-SIP-UA-MIB Enhancements Providing Functional Parity to SIP related CLI

The CISCO-SIP-UA-MIB Enhancements Providing Functional Parity to session initiation protocol (SII related CLI feature has Simple Network Management Protocol (SNMP)/command-line interface (CLI) MIB enhancements to maintain parity with SIP features released to date.

No documentation work is required. The MIB is “self-documenting.”

CNS Agents SSL Security

CNS Agents SSL Security is a Cisco IOS software feature that allows for the configuration of a secure connection between the CNS Agent, running on the Cisco IOS software-based device, and a CNS Server. Secure Socket Layer (SSL) encryption for CNS connections is enabled on the Cisco IOS device (CNS Agent) side using the **encrypt** keyword with the **cns config initial** or **cns config partial** global configuration mode commands.

Note This feature was originally introduced in Cisco IOS Release 12.1(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

CNS Configuration Agent

CNS is a foundation technology for linking users to network services. CNS SDK accomplishes this by making applications network-aware and increasing the intelligence of the network elements. CNS SDK provides building blocks to a range of customers in market segments such as Enterprise, service provider, independent software vendors, and system integrators.

The CNS Configuration Agent supports routing devices by providing:

- Initial configurations
- Incremental (partial) configurations
- Synchronized configuration updates

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcns_ca.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

CNS Event Agent

CNS is a foundation technology for linking users to network services. CNS SDK accomplishes this by making applications network-aware and increasing the intelligence of the network elements. CNS SDK provides building blocks to a range of customers in market segments such as Enterprise, service provider, independent software vendors, and system integrators.

The CNS Event Agent is part of the Cisco IOS infrastructure that allows Cisco IOS applications, for example CNS Configuration Agent, to publish and subscribe to events on a CNS Event Bus. CNS Event Agent works in conjunction with CNS Configuration Agent.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcns_ea.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Configuring a Gatekeeper to Provide Nonavailability Information for Terminating Endpoints

An H.323 Location Request (LRQ) message is sent by a gatekeeper to another gatekeeper to request a terminating endpoint. The second gatekeeper determines the appropriate endpoint on the basis of the information contained in the LRQ message. However, sometimes all the terminating endpoints are busy servicing other calls and none are available. If you configure the **lrq reject-resource-low** command, the second gatekeeper will reject the LRQ request if no terminating endpoints are available. If the command is not configured, the second gatekeeper will allocate and return a terminating endpoint address to the sending gatekeeper even if all the terminating endpoints are busy.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_lrqrj.htm.

Connect-Info RADIUS Attribute 77

The Connect-Info RADIUS Attribute 77 feature enables the network access server (NAS) to report Connect-Info (attribute 77) in accounting "start" and "stop" records that are sent to the RADIUS client. The "start" and "stop" records allow you to compare transmit and receive speeds and have a realistic view of a user session. Comparing transmit and receive speeds is important because many modem speeds are often different at the end of the modem connection (after negotiation).

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftattr77.htm.

Customer Profile Idle Timer Enhancements for Interesting Traffic

The Customer Profile Idle Timer Enhancements for Interesting Traffic feature supports a PPP idle timer based on interesting traffic for dialer interfaces.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftprfidl.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T as Interesting Traffic PPP and Customer Profile Idle Timer. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Default VPDN Group Template

The Default VPDN Group Template feature introduces the ability to configure global default values for virtual private dialup network (VPDN) parameters in a VPDN template. These global default values are applied to all VPDN groups, unless specific values are configured for individual VPDN groups. Previously, the Cisco IOS software required that VPDN parameters be configured for each individual VPDN group if the system default values were not desired.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdevpdn.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

DF Bit Override Functionality with IPSec Tunnels

The DF Bit Override Functionality with IPSec Tunnels feature allows customers to configure the setting of the DF bit when encapsulating tunnel mode IPSec traffic on a global or per-interface level. Thus, if the DF bit is set to clear, routers can fragment packets regardless of the original DF bit setting. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftdfipsc.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco AS5300 and Cisco AS5400 platforms.

DHCP Client—Dynamic Subnet Allocation API

The DHCP Client–Dynamic Subnet Allocation API feature is an application program interface (API) that is called by the DHCP Server–On-Demand Address Pool Manager feature for obtaining a subnet or releasing a subnet to the source server via DHCP. This feature allows automated configuration of layer 3 devices for simplified deployment.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

DHCP Client on WAN Interfaces

The DHCP Client on WAN Interfaces feature extends the Dynamic Host Configuration Protocol (DHCP) to allow PPP over ATM (PPPoA) and certain ATM interfaces to acquire an IP address through DHCP. By using DHCP rather than the IP Control Protocol (IPCP), a DHCP client can acquire other useful information such as DNS server addresses, the DNS default domain name, and default route.

Previously, the **ip address dhcp** interface configuration command could only be used on Ethernet interfaces. This feature allows the **ip address dhcp** command to be used on WAN interfaces.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftwandhp.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5800 platforms.

DHCP Relay—MPLS VPN Support

The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies. The DHCP relay agent information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent.

In some environments, a relay agent resides in a network element that also has access to one or more Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). A DHCP server that wants to offer service to DHCP clients on those different VPNs needs to know the VPN in which each client resides. The network element that contains the relay agent typically knows about the VPN association of the DHCP client and includes this information in the relay agent information option.

The DHCP Relay–MPLS VPN Support feature allows the relay agent to forward this necessary VPN-related information to the DHCP server using the following three suboptions of the DHCP relay agent information option:

- VPN identifier
- Subnet selection

- Server identifier override

The DHCP Relay–MPLS VPN Support feature enables a network administrator to conserve address space by allowing overlapping addresses. The relay agent can now support multiple clients on different VPNs, and many of these clients from different VPNs can share the same IP address.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdhmpls.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

DHCP Relay Agent Support for Unnumbered Interfaces

Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. Relay Agents receive Dynamic Host Configuration Protocol (DHCP) messages and then generate a new DHCP message to send out on another interface.

The Cisco IOS DHCP relay agent supports IP unnumbered interfaces. The DHCP relay agent automatically adds a static host route specifying the unnumbered interface as the outbound interface.

DHCP Server—On-Demand Address Pool Manager

The DHCP Server–On-Demand Address Pool Manager is a feature in which pools of IP addresses can be dynamically increased or reduced in size depending on the address utilization level. This feature supports address assignment using the Dynamic Host Configuration Protocol (DHCP) for customers using private addresses. Each on-demand address pool (ODAP) is configured and associated with a particular Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN).

When configured, the ODAP is populated with one or more subnets leased from a source server and is ready to serve address requests from DHCP clients or from PPP sessions. The source server can be a remote DHCP server or a RADIUS server (via AAA). Currently, only the Cisco Access Registrar RADIUS server supports ODAPs. Subnets can be added to the pool when a certain utilization level (high utilization mark) is achieved. When the utilization level falls below a certain level (low utilization mark), a subnet can be returned to the server from which it was originally leased.

This feature allows customers to optimize their use of IP addresses, thus conserving address space.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftondhcp.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

DHCP Server—Option to Ignore All BOOTP Requests

The DHCP Server—Option to Ignore All BOOTP Requests feature introduces the following new global configuration command: **ip dhcp bootp ignore**. This command allows the Cisco IOS DHCP server to ignore received BOOTP requests.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdbootp.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5400 platform.

Dialer CEF

The Dialer CEF feature introduces Cisco Express Forwarding (CEF) support for dialer interfaces. The Dialer CEF feature allows packets to be CEF switched across dialer interfaces rather than being low-end switched (LES) or fast switched. Compared to fast switching, CEF switching support improves switching performance by decreasing CPU utilization and lowering the packet loss rate. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftdlrcef.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300 and Cisco AS5400 platforms.

Dialer Persistent

The Dialer Persistent feature allows the connection settings in a dial-on-demand routing (DDR) dialer profile to be configured as *persistent*, that is, the connection is not torn down until the **shutdown** EXEC command is entered on the dialer interface. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftdperst.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 platforms.

Dialer Watch Connect Delay

The Dialer Watch Connect Delay feature introduces the ability to configure a delay in bringing up a secondary link when a primary link that is monitored by Dialer Watch goes down and is removed from the routing table. Previously, the router would instantly dial a secondary route without allowing time for the primary route to come back up. When the Dialer Watch Connect Delay feature is configured, the router will check for availability of the primary link at the end of the specified delay time before dialing the secondary link.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdialwl.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

Distributed Management Event and Expression MIB Persistence

The MIB Persistence feature allows the SNMP data of an MIB to be persistent across reloads; that is, MIB information retains the same set object values each time the user reboots. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmibpr1.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the Distributed Management Event MIB Persistence feature into the Cisco AS5300, Cisco AS5400, Cisco AS5800 platforms, and the Distributed Management Expression MIB Persistence feature into the Cisco AS5300 and Cisco AS5800 platforms.

Distributed Management Event MIB Conformance to RFC 2981

Prior to Cisco IOS Release 12.2(4)T3, Event MIB support in Cisco IOS software was based on the IETF internet draft version. In Cisco IOS Release 12.2(4)T3, the Cisco implementation of the EVENT-MIB was updated to comply with the finalized version of the Event MIB, as defined in RFC 2981. For detai see RFC 2981, available through the IETF web site at http://www.ietf.org.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T3. This release is porting the feature into the Cisco AS5300 and Cisco AS5400 platforms.

DLSw+ Enhanced Load Balancing

In a network with multiple capable paths, the Data Link Switch Plus (DLSw+) Load Balancing Enhancements feature improves traffic load balancing between peers by distributing new circuits based on existing loads and the desired ratio.

For each capable peer (peers that have the lowest or equal cost specified), the DLSw+ Load Balancing feature calculates the difference between the desired and the actual ratio of circuits being used on a peer. It detects the path that is underloaded in comparison to the other capable peers and assigns new circuits to that path until the desired ratio is achieved.

Note This feature was originally introduced in Cisco IOS Release 12.0(3)T. This release is porting the feature into the Cisco AS5350 platform.

DLSw+ Peer Group Clusters

The DLSw+ Peer Group Clusters feature reduces the explorer packet replication that typically occurs in a large Data Link Switch Plus (DLSw+) peer group design, where there are multiple routers connected to the same LAN.

The DLSw+ Peer Group Clusters feature associates DLSw+ peers (that are connected to the same LAN) into logical groups. Once the multiple peers are defined in the same peer group cluster, the DLSw+ Border Peer recognizes that it does not have to forward explorers to more than one member within the same peer group cluster.

Note This feature was originally introduced in Cisco IOS Release 12.0(3)T as DLSw+ Peer Clusters. This release is porting the feature into the Cisco AS5350 platform.

DTMF Events Through SIP Signaling

The DTMF Events Through SIP Signaling feature adds support for sending dual tone multifrequency (DTMF) notifications using NOTIFY messages from a session initiation protocol (SIP) gateway. The use of DTMF signaling for this feature enables support for advanced telephony services. Currently there are a number of application servers and service creation platforms that do not support media connections. To provide value added services to the network, these servers and platforms need to be aware of signaling events from a specific participant in the call. After the server or platform is aware of the DTMF events that are being signaled, it can use third-party call control, or other signaling mechanisms, to provide enhanced services. Examples of the types of services and platforms that are supported by this feature are various voice web browser services, Centrex switches/business service platforms, calling card services, and unified message servers. All of these applications require a method for the user to communicate with the application outside of the media connection. The Preauthentication with ISDN PRI feature provides this signaling capability.

The output generated by the **show sip-ua statistics** command displays the enhanced SIP Response and Total Traffic Statistics available with the new feature.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftnotify.htm.

DTMF Relay for SIP calls Using Named Telephone Events

The DTMF Relay using Named Telephone Events feature adds support for relaying dual tone multifrequency (DTMF) tones and hookflash events in session initiation protocol (SIP) on Cisco Voice over IP (VoIP) gateways (note that this feature is implemented for SIP only). Using Named Telephone Events (NTE) to relay DTMF tones provides a standardized means of transporting DTMF tones in RTP packets according to section 3 of RFC 2833, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, developed by the Internet Engineering Task Force (IETF) Audio/Video Transport (AVT) working group. RFC 2833 defines formats of NTE RTP packets used to transport DTMF digits, hookflash, and other telephony events between two peer endpoints.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_dtmf.htm.

Easy VPN Server

The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x software clients and Cisco VPN hardware clients. It allows a remote end user to communicate using IP Security (IPSec) with any Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "pushed" to the client by the server, minimizing configuration by the end user.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftunity.htm.

6746

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Enable Multilink PPP via RADIUS for Preauthentication User

The Enable Multilink PPP via RADIUS for Preauthentication User feature allows you to selectively enable and disable Multilink PPP (MLP) negotiation for different users via RADIUS vendor-specific attribute (VSA) preauth:ppp-multilink=1.

You can enable MLP by configuring the **ppp multilink** command on an interface, but then this command enables MLP negotiation for all connections and users on that interface; that is, you cannot selectively enable or disable MLP negotiation for specific connections and users on an interface.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftppprad.htm

Encrypted Vendor-Specific Attributes

The Encrypted Vendor-Specific Attributes feature introduces support for the following three types of string vendor-specific attributes (VSAs):

- Tagged string VSA—To retrieve the right value for this VSA, the Tag field must be parsed correctly. The value for this field can range only from 0x01 through 0x1F. If the value is not within the specified range, the RADIUS server will ignore the value and consider the Tag field to be a part of the attribute string field.
- Encrypted string VSA—This VSA has a Salt field that ensures the uniqueness of the encryption key that is used to encrypt each instance of the VSA. The first and most significant bit of the Salt field must be set to 1.
- Tagged and Encrypted string VSA—This VSA is similar to encrypted string VSAs *except* this VSA has an additional Tag field. If the Tag field is not within the valid range (0x01 0x01 through 0x1F), it is considered to be part of the Salt field.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftencvsa.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the featu into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

Enhanced Codec Support for SIP Using Dynamic Payloads

The Enhanced Codec Support for SIP Using Dynamic Payloads feature enhances codec selection and payload negotiation between originating and terminating session initiation protocol (SIP) gateways. The Enhanced Codec Support for SIP Using Dynamic Payloads feature provides the following SIP enhancements:

- Additional codec support
- Dynamic payload configuration
- Enhanced SDP messages

The feature adds support, which varies on different platforms, for eight additional codecs:

- Clear-channel
- G723ar53
- G723ar63
- G723r53
- G726r16
- G726r24
- G729br8
- GSM-EFR

The feature adds support for dynamic payloads by expanding SIP ability to advertise and negotiate available codecs. The feature also expands the Session Description Protocol (SDP) message body of SIP INVITE requests, which describe codec capabilities of the SIP gateway.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftcodec.htm.

Enhanced Debug Capabilities for Cisco Voice Gateways

The Enhanced Debug Capabilities for Cisco Voice Gateways feature provides a uniform call identifier to track calls end-to-end, filter calls based on certain criteria, and provide more concise debug commands. Previously if all debugs were turned on, the debug output would wrap around, so viewing a smaller amount of debug output to effectively identify the problem areas was critical.

Another requirement was single-call tracing that enables a single call, based on certain criteria, to be traced end-to-end in the gateway. A generic format to identify the trace call was required also and was needed across Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), H.323, voice telephony service providers (VTSPs), session applications, interactive voice response (IVR), Call Control Applications Programming Interface (CCAPI) and digital signal processors (DSPs).

The voice call debug command was implemented to give the user the choice of displaying the full GUID or reduces the length of GUID by displaying the headers only. The **full-guid** keyword displays a full call trace and the default is displaying the header only.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_dbgsy.htm

Enhanced Password Security

The Enhanced Password Security feature allows you to configure Message Digest 5 (MD5) encryption for username passwords. Before the introduction of this feature, there were two types of passwords associated with usernames: Type 0, which is a clear text password visible to any user who has access to privileged mode on the router, and type 7, which is a password with a weak, exclusive, or type encryption. Type 7 passwords can be retrieved from the encrypted text by using publicly available tools.

Use the **username secret** command to configure a username and an associated MD5-encrypted secret.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_md5.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

Enhanced Test Command

The Enhanced Test Command feature introduces two new commands—**aaa user profile** and **aaa attribute**—that allow you to create a named user profile with calling line identification (CLID) or dialed number identification service (DNIS) attribute values, which can be associated with a **test aaa group** command.

Use the **aaa attribute** command to add CLID or DNIS attribute values to a user profile, which is created by using the aaa user profile command. The CLID or DNIS attribute values can be associated with the record that is going out with the user profile (via the test aaa group command), thereby providing the RADIUS server with access to CLID or DNIS attribute information for all incoming calls. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftaaacmd.ht

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Enhanced VoiceXML Diagnostics

With the Enhanced VoiceXML Diagnostics feature, debugging output can be filtered for all VoiceXML applications except the application named in the **debug condition application voice** command. When this command is configured, the gateway displays debugging messages only for the specified VoiceXML application when using the **debug vxml** and **debug http client** commands.

Refer to the following documents for additional information:

- Cisco IOS TCL and VoiceXML Application Guide:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ivrapp/index.htm.

- Cisco VoiceXML Programmer's Guide:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/vxmlprg/index.htm.

Enhancements for the Cisco VG200 Voice Gateway

The Enhancements for the Cisco VG200 Voice Gateway feature provides the Cisco VG200 platform with increased voice gateway feature parity to the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series. This feature is also supported on the Cisco VG200XM platform upgrade. The Cisco VG200XM is new for Cisco IOS Release 12.2(11)T and is a more powerful version of the Cisco VG200, offering higher processing power and improved performance.

The Cisco VG200 platforms provide the following default memory options:

- CiscoVG200—8 MB of Flash, 64 MB of DRAM
- Cisco CG200XM—16 MB of Flash, 64 MB of DRAM

The Enhancements for the Cisco VG200 Voice Gateway feature includes the following features:

- FXO Answer and Disconnect supervision—Enables analog Foreign Exchange Office (FXO) ports to monitor call-progress tones and to monitor voice and fax transmissions returned from a PBX or from the Public Switched Telephone Network (PSTN).
- NM-HDV-1T1/E1-12 —This digital voice card provides telephony interface signaling support, providing a lower density digital solution.
- Private-line automatic ringdown (PLAR)—Provides an off-premises extension (OPX) from a private PBX. Also provides dial tone from a remote PBX.
- Proprietary Transfer Code—Enables the Cisco VG200 (acting as a PSTN gateway with an Survivable Remote Site Telephony (SRST) or ITS device) to support Cisco proprietary call transfer from the SRST or ITS device back to the PSTN.

Enhancing Raw Buffer Management: Audit and Prepopulation for Channel-Associated Signaling

This feature implements an audit process to reclaim leaking raw buffers on a channel-associated signaling (CAS) interface.

Buffers pass voice data between subsystems in a voice-call-control infrastructure. However, pool management and the improper usage of buffers result in either process memory exhaustion or system crashes. Both are relatively difficult to troubleshoot. Auditing raw buffers allows you to detect and reclaim leaking buffers on the CAS interface and thus to improve buffer availability and be memory efficient.

Auditing raw buffers provides the following monitor scheme: When a raw message is allocated, the start time stamp is recorded. An audit process periodically (every 2 minutes) reclaims active raw messages that are more than 10 minutes old and returns the buffers to the appropriate pool. The 10-minute window allows enough time for all the call-related events to pass through.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftrawr11.htm

Event Tracer

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, route processor switchover.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s18/evnttrcr.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Fax and Modem Pass-Through over VoIP

Fax and modem pass-through are supported on the Cisco 2600 series, Cisco 3600 series, and the Cisco 3700 series modular access routers beginning in Cisco IOS Release 12.2(11)T.

Note The Fax and Modem Pass-Through over VoIP feature is also known under the feature title Modem Passthrough over Voice over IP.

On detection of the fax or modem tone on an established VoIP call, the gateways switch into modem fax or pass-through mode: the voice codec and configuration is suspended and the pass-through parameters are loaded for the duration of the fax or modem session. This changes the bandwidth needed for the call to the equivalent of G.711.

With pass-through, the fax or modem traffic is carried between the two gateways in RTP packets, using an uncompressed format resembling the G.711 codec. Packet redundancy may be used to mitigate the effects of packet loss in the IP network. Even so, fax and modem pass-through remain susceptible to packet loss, jitter and latency in the IP network. The two endpoints must be clocked synchronously for this type of transport to work predictably.

The Fax and Modem Pass-Through feature is also known as Voice Band Data (VBD) by the International Telecommunication Union (ITU). VBD refers to the transport of fax or modem signals over a voice channel through a packet network with an encoding appropriate for fax or modem signals. The minimum set of coders for VBD mode is G.711 ulaw and alaw with VAD disabled. For modem transport, Ech cancellation is also be disabled.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/index.htm.

Fax Detection (Single-number Voice and Fax)

Note The Fax Detection (Single-number Voice and Fax) feature is also known under the feature title Fax Detection for Cisco AS5300, Cisco AS5350 and Cisco AS5400.

On Cisco AS5300, Cisco AS5350, and Cisco AS5400 gateways that are equipped with voice feature cards (VFCs), the fax detection feature lets service providers deploy unified communication applications in which each subscriber has a single E.164 number for both voice mail and fax mail. When configured for fax detection, the gateway automatically listens to incoming calls to discriminate between voice and fax. The gateway then routes the calls to the appropriate application or server.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/ind.htm.

Fax Detection for VoiceXML

With the Fax Detection for VoiceXML feature, when a VoiceXML fax detection application is configured on the gateway, callers can dial a single number for both voice and fax calls. The gateway automatically detects that a call is a fax transmission by listening for comfort noise generation (CNG), the distinctive fax "calling" tone. When configured for fax detection, the Cisco VoiceXML gateway continuously listens to incoming calls to determine which calls are voice or fax. The gateway then routes the calls to the appropriate application or media server.

Refer to the following documents for additional information:

- Cisco IOS TCL and VoiceXML Application Guide:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ivrapp/index.htm.

- Cisco VoiceXML Programmer's Guide:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/vxmlprg/index.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)XB on the Cisco AS5300 platform. This release is porting the feature into the Cisco 3640 series, Cisco 3660 series, Cisco AS5350, and Cisco AS5400 platforms.

Fax Relay Packet Loss Concealment

The Fax Relay Packet Loss Concealment feature improves the current real-time fax over IP (commonly known as fax relay) implementation in Cisco gateways, allowing fax transmissions to work reliably over higher packet loss conditions.

In addition, this feature includes enhanced real-time fax debug capabilities and statistics. These debugs and statistics will give better visibility into the real-time fax operation in the gateway, allowing for improved field diagnostics and troubleshooting.

These improvements include configuration of fax relay Error Correction Mode (ECM) on the Voice over IP (VoIP) dial peer. ECM provides for error-free page transmission. This mode is available on fax machines that include memory for storage of the page data (usually high-end fax machines).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_0393.htm.

Note This feature was previously released in Cisco IOS Release 12.1(3)T on the Cisco AS5300 and Cisco AS5850 platforms. This release is porting the feature into the Cisco AS5400 platform.

G.Clear, GSMFR, and G.726 Codecs and Modem and Fax Pass-Through for Cisco Universal Gateways

The following features are now available on Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5400HPX, and Cisco AS5850 universal gateways.

The G.Clear, GSMFR, and G.726 Codecs and Modem and Fax Pass-Through for Cisco Universal Gateways feature provides support for G.Clear, GSMFR, and G.726 codecs, as well as support for modem and fax Pass-through for Cisco universal gateways.

G.Clear guarantees bit integrity when transferring a DS-0 through a gateway server, supports the transporting of nonvoice circuit data sessions through a Voice over IP (VoIP) network, and enables the VoIP networks to transport ISDN and switched 56 circuit-switched data calls. With the availability of G.Clear, ISDN data calls that do not require bonding can be supported.

The GSMFR codec was introduced in 1987. The GSMFR speech coder has a frame size of 20 ms and operates at a bit rate of 13 kbps. GSMFR is an Regular Pulse Excited - Linear Predictive (RPE-LTP) coder.

The G.726 Adaptive Differential PCM (ADPCM) voice codec operates at bit rates of 16, 24, and 32 kbps. ADPCM provides the following:

- Voice mail recording and playback that is a requirement for Internet voice mail.

- Voice transport for cellular, wireless, and cable markets.
- High voice quality voice transport at 32 kbps.

In addition, modem and fax pass-through services are supported. When service providers and aggregators are implementing VoIP, they sometimes cannot separate fax or data traffic from voice traffic. These carriers that aggregate voice traffic over VoIP infrastructures require service offerings to carry fax and data as easily as voice.

On detection of the modem answer tone, the gateways switch into modem pass-through mode. With modem pass-through, the modem traffic is carried between the two gateways in RTP packets, using an uncompressed or lightly compressed voice codec—G.711 ulaw, G.711 alaw, or Voice Band Data (VBD). Packet redundancy may be used to mitigate the effects of packet loss in the IP network. Even so, modem pass-through remains susceptible to packet loss and jitter and latency in the IP network.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_ghost.htm.

Gatekeeper Endpoint Control Enhancements

The Gatekeeper Endpoint Control Enhancements feature provides enhancements to the Cisco IOS gatekeeper, including commands to allow both forced unregistration of an endpoint and rejection of new registrations or calls when a Gatekeeper Transaction Message Protocol (GKTMP) server is down or unreachable. This feature also provides both forced unregistration of an endpoint using a GKTMP command from an application server and a command to enable faster reconnection to a GKTMP server when its TCP connection fails.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftgkece2.htm

Gatekeeper-to-Gatekeeper Authentication

The Gatekeeper-to-Gatekeeper Authentication feature provides additional security for H.323 networks by introducing the ability to validate intra-domain and interdomain gatekeeper-to-gatekeeper Location Request (LRQ) messages on a per-hop basis. When used in conjunction with per-call security using the interzone ClearToken (IZCT), network resources and security holes are protected from hackers. The IZCT was introduced in the Inter-Domain Gatekeeper Security Enhancement feature released in Cisco IOS Release 12.2(2)XA and Cisco IOS Release 12.2(4)T.

The Gatekeeper-to-Gatekeeper Authentication feature provides a Cisco Access Token (CAT) to carry authentication within zones. The CAT is used by adjacent gatekeepers to authenticate each other and configured on a per-zone basis. In addition, service providers can specify inbound passwords to authenticate LRQ messages coming from foreign domains and outbound passwords to be included in LRQ messages to foreign domains.

This release documents two new commands: **security password-group** and **security zone**.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_idlrq.htm.

Generic Routing Encapsulation (GRE) Tunnel Keepalive

The GRE Tunnel Keepalive feature provides the capability of configuring keepalive packets to be sent over IP-encapsulated generic routing encapsulation (GRE) tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/grekpliv.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

Global Modem Counters

The Global Modem Counters feature adds two new global call counters for ISDN calls to the Cisco IOS software. In Cisco IOS Release 12.2(11)T, this feature is supported only on the Cisco AS5800 universal access server. The CISCO-POP-MGMT-MIB has been updated with two new objects, cpmCallVolSuccISDNDigital and cpmCallVolAnalogCallClearedNormally. The cpmCallVolSuccISDNDigital object allows the Cisco IOS software to track the number of successful incoming and outgoing ISDN digital data calls that have occurred since the system was started. The cpmCallVolAnalogCallClearedNormally object allows the Cisco IOS to track the number of successful incoming and outgoing analog data calls.

No new commands have been introduced with this feature. To use this feature, enable System Network Management Protocol (SNMP) and the corresponding OIDs for these new objects. To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Globalized Cadence and Tone for Cisco IOS Gateways

Because previously Cisco CallManager and Cisco IOS gateways were configured independently and may lead to configuration mismatches, Cisco CallManager is now preconfigured to provide cadences and tones for the user's locale. It is no longer necessary for you to configure the **cptone** command on the gateway. This feature shows the user how to verify which locale is preconfigured on Cisco CallManager.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_glbl.htm.

GTD for GKTMP using SS7 Interconnect version 2.0

The GTD for GKTMP using SS7 Interconnect version 2.0 feature consists of the following two features:

- GTD for GKTMP using SS7 Interconnect for Voice Gatekeeper version 2.0
- GTD for GKTMP using SS7 Interconnect for Voice Gateway version 2.0

The GTD for GKTMP Using SS7 Interconnect version 2.0 feature provides additional functionality to Cisco gateways and gatekeepers in a Cisco SS7 Interconnect for Voice Gateways Solution. The generic transparency descriptor or generic telephony descriptor (GTD) format is defined in the a Cisco proprietary draft. GTD format defines parameters and messages of existing SS7 ISUP protocols in text format and allows SS7 messages to be carried as a payload in the H.225 registration, admission, and status (RAS) messages between the GW and GK. GTD messages can also be transported between GWs and GKs in H.323 messages. With the GTD feature, the GK extracts the GTD message and the external route server derives routing and accounting information based upon the GTD information provided from the Cisco Gatekeeper Transaction Message Protocol (GKTMP).

Currently routing on Cisco GWs is based on generic parameters such as originating number, destination number, and port source. Adding support for SS7 ISUP messages allows the VoIP network to use additional routing enhancements found in traditional TDM switches.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftgtdpy2.htm

H.323 Call Redirection Enhancements

The user-to-user information element (UUIE) of the Facility message is used primarily for call redirection. The UUIE contains a field, facilityReason, that indicates the nature of the redirection. The H.323 Call Redirection Enhancements feature adds support for two of the reasons: routeCallToGatekeeper and callForwarded. It also provides a nonstandard method for using the Facil message to effect call transfer.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftcallrd.htm.

Note This feature was previously released in Cisco IOS Release 12.2(2)T on Cisco 1700, Cisco 2600 series, Cisco 3600 series, Cisco MC3810, Cisco AS5300, and Cisco uBR924 platforms. This release is porting the feature into the Cisco AS5850 platform.

H.323 Dual Tone Multifrequency (DTMF) Relay Using Named Telephone Events

Until now, the Named Telephone Event (NTE) method of dual tone multifrequency (DTMF) relay was available on Cisco gateways only for Session Initiation Protocol (SIP) and Media Gateway Control Protocol (MGCP) gateways. The H.323 Dual Tone Multifrequency Relay Using Named Telephone Events feature adds support for this method for H.323 gateways.

Cisco H.323 gateways advertise capabilities using the H.245 capabilities messages. By default, they advertise that they can receive all DTMF relay modes. If the capabilities of the remote gateway do not match, the Cisco H.323 gateway transmits DTMF tones as in-band voice. Configuring DTMF relay o the Cisco H.323 gateway sets preferences for how the gateway handles DTMF transmission. If multiple methods are configured, the priority is as follows:

- Cisco RTP
- RTP NTE
- H.245 signal
- H.245 alphanumeric

In addition to support for NTE, the H.323 Dual Tone Multifrequency Relay Using Named Telephone Events feature provides support for asymmetrical payload types. Payload types can differ between local and remote endpoints. Therefore, the Cisco gateway can transmit one payload type value and receive a different payload type value.

There are no new or modified commands.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/fth3dtmf.htm

H.323 Redundant Zone Support

The Redundant H.323 Zone Support feature allows users to configure multiple gatekeepers to service the same zone or technology prefix. This feature can be used with the Gateway Support for Alternate Gatekeepers feature, which allows a user to configure a gateway to point to two gatekeepers (one as the primary and the other as the alternate). Together, these features allow a user to configure a Cisco gateway to send location requests (LRQs) to two or more Cisco gatekeepers—one as a primary and the others as back up gatekeepers. All gatekeepers are active. The gateway can choose to register with any one (but not all) at a given time.

Note This feature was previously released in Cisco IOS Release 12.1(1)T. This release is porting the feature into the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

iBGP Multipath Load Sharing

When a Border Gateway Protocol (BGP) speaker router with no local policy configured receives multiple network layer reachability information (NLRI) from the internal BGP for the same destination, the router will choose one internal BGP path as the best path. The best path is then installed in the IP routing table of the router.

The Internal BGP Multipath Load Sharing feature enables the BGP speaker router to select multiple internal BGP paths as the best paths to a destination. The best paths or multipaths are then installed in the IP routing table of the router.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11bmls.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

IGMP MIB Support Enhancements for SNMP

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to neighboring multicast routers. The IGMP MIB describes objects that enable users to remotely monitor and configure IGMP using Simple Network Management Protocol (SNMP). It also allows users to remotely subscribe and unsubscribe from multicast groups. The IGMP MIB Support Enhancements for SNMP feature adds full support of RFC 2933 (Internet Group Management Protocol MIB) in Cisco IOS software. There are no new or modified Cisco IOS commands associated with this feature.

For complete details on the IGMP MIB, see the IGMP-STD-MIB.my file available from the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

IKE—Initiate Aggressive Mode

The IKE—Initiate Aggressive Mode feature allows you to specify RADIUS Tunnel attributes (Tunnel-Client-Endpoint [66] and Tunnel-Password [69]) for an IPSec peer and to initiate an IKE aggressive mode negotiation with the tunnel attributes. This feature is best implemented in a crypto hub-and-spoke scenario, in which the spokes initiate IKE aggressive mode negotiation with the hub by using the preshared keys that are specified as tunnel attributes and stored on the AAA server. This scenario is scalable because the preshared keys are kept at a central repository (the AAA server) and more than one hub router and one application can use the information.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ikeag.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Integrated Signaling Link Terminal

The Integrated Signaling Link Terminal feature pulls existing Cisco distributed Message Transfer Part (MTP) SS7 signaling architecture functionality—previously available only on Cisco 26*xx*-based signaling link terminals (SLTs)—directly onto a single Cisco AS5350 or Cisco AS5400. Like the Cisco 26*xx*-based SLT, the Integrated SLT on a Cisco AS5350 or Cisco AS5400 backhauls upper-layer Signaling System 7 (SS7) protocols across an IP network using Cisco Reliable User Datagram Protocol (RUDP), terminating the MTP1 and MTP2 layers of the SS7 protocol stack at the Media Gateway Controller (MGC).

Using the 2-, 4-, or 8-PRI dial feature card (DFC) or the CT3 (28-PRI) DFC card, this feature is designed for small points of presence (POPs) that require only one or two network access servers (NASs) or Voice-over-IP (VoIP) gateways as part of a dial or VoIP solution. This feature eliminates the use of the Cisco 26*xx*-based SLT in the product configuration.

When the Integrated Signaling Link Feature feature is implemented, a Cisco AS5350 or Cisco AS5400 functions as an SS7 signaling data link terminal and as a NAS, voice gateway, or both when universal ports are used.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftintslt.htm.

Integrated IS-IS Point-to-Point Adjacency Over Broadcast Media

When a network consists of only two networking devices that are connected to broadcast media and using the integrated IS-IS protocol, it is better for the system not to have to handle the link as a broadcast link but rather as a point-to-point link. The Integrated IS-IS Point-to-Point Adjacency Over Broadcast Media feature introduces a new command to make IS-IS behave as a point-to-point link between the networking devices. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftissp2p.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Interactive Voice Response Version 2.0 on VoIP Gateways

Interactive Voice Response (IVR) consists of simple voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination. IVR applications can be assigned to specific ports or invoked on the basis of dialed number identification service (DNIS). An IP Public Switched Telephone Network (PSTN) gateway can have several IVR applications to accommodate many different gateway services, and you can customize the IVR applications to present different interfaces to the various callers.

IVR systems provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words, or more commonly, dual tone multifrequency (DTMF) signaling. IVR uses Tool Command Language (TCL) scripts to gather information and to process accounting and billing.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ivr72.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(3)T. This release is porting the feature into the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

Inter-Domain Gatekeeper Security Enhancement

The Inter-Domain Gatekeeper Security Enhancement feature provides a means of authenticating and authorizing H.323 calls between the administrative domains of Internet Telephone Service Providers (ITSPs).

An interzone ClearToken (IZCT) is generated in the originating gatekeeper (OGK) when a location request (LRQ) is initiated or an admission confirmation (ACF) is about to be sent for an intrazone call within an ITSP's administrative domain. As the IZCT traverses the routing path, each gatekeeper (GK) stamps the IZCT's destination GK ID with its own ID. This identifies when the IZCT is being passed over to another ITSP's domain. The IZCT is then sent back to the OGW in the location confirmation (LCF) message. The OGW passes the IZCT to the terminating gateway (TGW) in the SETUP message. The TGW forwards the IZCT in the admission request (ARQ) answerCall field to the terminating gatekeeper (TGK), which then validates it.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_ctoke.htm.

Interface Alias Long Name Support

The Interface Alias (ifAlias) is a user-specified description of an interface used for SNMP network management. The ifAlias is an object in the Interfaces Group MIB (IF-MIB), which can be set by a network manager to "name" an interface. The ifAlias value for an interface or subinterface can be set using the **description** command in interface configuration mode, or by using a Set operation from a Network Management System.

Before Cisco IOS Release 12.2(2)T, ifAlias descriptions for subinterfaces were limited to 64 characters. A new Cisco IOS software command, **snmp ifmib ifalias long**, configures the system to handle ifAlias descriptions of up to 256 characters. IfAlias descriptions appear in the output of the **show interfaces** CLI command. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftshowif.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Interface Index Display

The Interface Index (IfIndex) is a user-specified identification number for an interface used in SNMP network management. The IfIndex is an object in the Interfaces Group MIB (IF-MIB), which can be set by a network manager to consistently identify an interface. A new Cisco IOS software command, **show snmp mib ifmib ifindex**, allows the user to display the IfIndex identification numbers assigned to interfaces and subinterfaces using the CLI. The IFIndex provides a way to display these values without the need for a Network Management Station. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftshowif.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Internal Cause Code Consistency Between SIP and H.323

The Internal Cause Code Consistency Between SIP and H.323 feature establishes a standard set of categories for internal causes of voice call failures. Before this feature, the cause code passed when an internal failure occurred was not standardized or based on any defined rules. The nonstandardization led to confusing or incorrect cause code information, and possibly contributed to billing errors.

The H.323 and SIP standard cause codes that are now generated accurately reflect the nature of each internal failure. This makes H.323 and SIP consistent with cause codes generated for common problems. Also, for each internal failure, an ITU-T Q.850 release cause code is also assigned.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftbibble.htm.

Interworking of Cisco MGCP Voice Gateways and Cisco CallManager Version 3.2

The Interworking of Cisco MGCP Voice Gateways and Cisco CallManager Version 3.2 feature allows Cisco voice gateways to act as redundant fail-over MGCP gateways. The new functionality includes the following configurable options:

- Cisco CallManager Redundancy—A fallback Cisco CallManager instance can assume control of the backup voice gateways in the event of a failure; another pair of resources can be specified for use in case the primary fallback Cisco CallManager also fails.
- Supplementary Services—During a fail-over event, call hold, call transfer when the line is busy or there is no answer, call forwarding, and three-party call conferencing to and from the Public Switched Telephone Network (PSTN) or a private branch exchange (PBX) are supported.
- Cisco CallManager Switchback—This feature allows reestablishment of communication with the primary Cisco CallManager when it becomes available after fallback resources have assumed control.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_ccm1.htm.

Interworking Signaling Enhancements for H.323 and SIP VoIP

The Interworking Signaling Enhancements for H.323 and SIP VoIP feature enables VoIP networks to properly signal the setup and tear-down of calls when interworking with PSTN networks. These enhancements ensure that in-band tones and announcements are generated when needed so that the voice path is cut-through at the appropriate point of call setup and that early alerting (ringing) does not occur. In addition, support for network-side ISDN and the reducing of speech clipping is addressed.

Note This feature was originally introduced in Cisco IOS Release 12.1(5)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

IP Multicast MIB Enhancements

This feature enhances the IP multicast routing protocol in Cisco IOS software by adding MIB variables to query the number of (S, G) and (*, G) entries. It also adds support for high-speed interface counters.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

IPSec VPN High Availability Enhancements

The IPSec VPN High Availability feature consists of two new features—Reverse Route Injection and Hot Standby Router Protocol and IPSec—that work together to provide users with a simplified network design for VPNs and reduced configuration complexity on remote peers with respect to defining gateway lists.

Reverse Route Injection

Reverse Route Injection (RRI) is a feature designed to simplify network design for Virtual Private Network (VPNs) in which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

In the dynamic case, as remote peers establish IPSec security associations (SAs) with an RRI-enabled router, a static route is created for each subnet or host protected by that remote peer. For static crypto maps, a static route is created for each destination of an extended access-list rule.

When routes are created, they are injected into any dynamic routing protocol and distributed to surrounding devices. This traffic flows, requiring IPSec to be directed to the appropriate RRI router for transport across the correct SAs to avoid IPSec policy mismatches and possible packet loss.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco 1760 series router and the Cisco AS5300 and Cisco AS5050 platforms.

Hot Standby Router Protocol and IPSec

Hot Standby Router Protocol (HSRP) is designed to provide high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. HSRP is particularly useful for hosts that do not support a router discovery protocol, such as ICMP Router Discovery Protocol (IRDP), and do not have the functionality to switch to a new router when their selected router reloads or loses power. Without this functionality, a router that loses its default gateway because of a router failure is unable to communicate with the network.

HSRP is configurable on LAN interfaces using standby command line interface (CLI) commands. It is now possible to use the standby IP address from an interface as the local IPSec identity, or local tunnel endpoint.

By using the standby IP address as the tunnel endpoint, failover can be applied to VPN routers by using HSRP. Remote VPN gateways connect to the local VPN router via the standby address that belongs to the active device in the HSRP group. In the event of failover, the standby device takes over ownership of the standby IP address and begins to service remote VPN gateways.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco 1760 series router and the Cisco AS5300 and Cisco AS5050 platforms.

Further Documentation

Refer to the following document for further information about the IPSec VPN High Availability Enhancements feature:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e9/ipsecha.htm.

IPv6 for Cisco IOS Software

IPv6, formerly called IPng (next generation), is a replacement for the current version of IP (version 4). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/index.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300 and Cisco AS5400 platforms.

ISDN and V.120 Support for NextPort DSPs

The ISDN and V.120 Support For NextPort DSPs feature provides full coverage for digital calls and performance enhancement for V.120 calls. The feature permits terminating synchronous ISDN and V.120 sessions without customer intervention. This feature allows the Cisco AS5350 and Cisco AS5400 to terminate more than 256 ISDN sessions per channelized T3 (CT3) controller by adding ISDN capacity. This feature is mandatory for wholesale dial installations in which ISDN is being used. Th. feature permits V.120 calls to operate on the NextPort digital signal processor (DSP) instead of on the CT3 controller to reduce activity on the CPU and to increase the V.120 call capability. Support for these enhancements is automatic, and no configuration steps are required.

ISDN-NFAS with D Channel Backup

ISDN Non-Facility Associated Signaling (NFAS) allows a single D channel to control multiple PRI interfaces. A backup D channel can be configured for use when the primary NFAS D channel fails. Any hard failure causes a switchover to the backup D channel and currently connected calls remain connected. The ISDN-NFAS with D Channel Backup feature also supports the DMS100 and NI2 switch types.

Once the channelized T1controllers are configured for ISDN PRI, only the NFAS primary D channel must be configured; its configuration is distributed to all the members of the associated NFAS group.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5800/sw_conf/ios_122/ft_nfas.htm.

Note This feature was originally introduced in Cisco IOS Release 11.3(3)T. This release is porting the feature into the Cisco AS5850 platform. Note that the feature is also known as NFAS with D Channel Backup.

IVR: Configuring Dynamic Prompts

The functionality of dynamic prompts, an existing Cisco IOS feature, has been expanded in Cisco IOS Release 12.2(11)T to play out International Organization for Standardization (ISO) formatted time and date, and visible noncontrol ASCII characters. Dynamic prompts allow a TCL application to play the date and time information on a Cisco voice gateway. The information is first retrieved by using the **clock** command in the Toolkit Command Language (TCL) library and then played through dynamic prompts using the multilanguage script.

The **media play** command in the TCL library plays the specified dynamic prompt on the specified call leg. The English version of the multilanguage TCL script must be enabled before you use the **media play** command; it allows a dynamic prompt to play string and visible noncontrol ASCII characters.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/actap/index.htm.

IVR: Customizing Accounting Templates

You can create an accounting template to customize your accounting records based on your billing needs. An accounting template is a text-based interface that allows you to customize and define the content of that template and helps reduce billing traffic from the gateway to the accounting servers.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/actap/index.htm.

IVR: Directing AAA Requests

Cisco IOS Release 12.2(11)T introduces the capability of splitting authentication, authorization, and accounting (AAA) requests to RADIUS servers based on account number, called party number, and incoming trunk groups.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/actap/index.htm.

IVR: Enhanced Multilanguage Support

This feature releases the infrastructure to support Tool Command Language (TCL)-based script interpreters, which allow you to easily add new languages to your router or access server. You can add a new language by creating a TCL script that interprets prompts into a sequence of audio files or silences. The underlying Cisco IOS dynamic prompting code interfaces with the TCL script to translate the message into a sequence of URLs that point to audio files. Then, the Cisco IOS software plays the sequence of audio files as a dynamic prompt. New TCL-script language interpreters operate simultaneously with the current built-in languages: Spanish, Chinese/Mandarin, and English. Adversely, new TCL-script language interpreters can replace one or more of the built-in languages by overwriting the built-in language functionality.

Note This feature does not release any specific TCL scripts.

Note Although the language intelligence comes from a TCL-based language script, once you configure a language any system (TCL IVR 1.0, 2.0, VxML, MGCP, and so on) on your router can use the configured language with little to no change to Cisco IOS Software.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmultil.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T as Enhanced Multilingual Support for Cisco IOS Integrated Voice Response. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

L2TP Large-Scale Dial-Out

The L2TP Large-Scale Dial-Out feature enables the router to dial multiple Layer 2 Tunnel Protocol (L2TP) access concentrators (LACs) from a single L2TP network server (LNS). The LACs are signaled through the LNS and use L2TP to establish the dial sessions. User-defined profiles can be configured on an authentication, authorization, and accounting (AAA) server and retrieved by the LNS when dial-out occurs.The L2TP Large-Scale Dial-Out feature also supports multiple LACs bound into one stack group, call traffic load balancing, and outbound call congestion management.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftl2lsdo.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

L2TP Security

The L2TP Security feature provides enhanced security for tunneled PPP frames between the Layer 2 Transport Protocol (L2TP) access concentrator (LAC) and the L2TP network server (LNS). Previous releases of the Cisco IOS software provided only a one-time, optional mutual authentication during tunnel setup with no authentication of subsequent data packets or control messages. In situations in which the L2TP is used to tunnel PPP sessions over an untrusted infrastructure such as the Internet, the security attributes of L2TP and PPP are inadequate. PPP provides no protection of the L2TP tunnel, and current PPP encryption protocols provide inadequate key management and no authentication or integrity mechanisms. The L2TP Security feature allows the robust security features of IP Security (IPSec) to protect the L2TP tunnel and the PPP sessions within the tunnel. In addition, the L2TP Security feature provides built-in keepalives and standardized interfaces for user authentication and accounting to authentication, authorization, and accounting (AAA) servers.

The deployment of Microsoft Windows 2000 demands the integration of IPSec with L2TP because this is the default virtual private dialup network (VPDN) networking scenario. This integration of protocols is also used for LAN-to-LAN VPDN connections in Microsoft Windows 2000. The L2TP Security feature provides integration of IPSec with L2TP in a solution that is scalable to large networks with minimal configuration.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftl2tsec.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400 and Cisco AS5800 platforms.

Location Confirmation (LCF) Enhancements for Alternate Endpoints

This feature was originally introduced in Cisco IOS Release 12.2(4)T; see the "Location Confirmation Enhancements for Alternate Endpoints" section on page 370. Cisco IOS Release 12.2(11)T documents the new **endpoint alt-ep collect** command. In addition, effective with Cisco IOS Release 12.2(11)T, duplicate alternate endpoints that are received in a Location Confirmation (LCF) message are removed from the consolidated list of endpoints.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_lcfep.htm.

Low Latency Queueing with Priority Percentage Support

This feature allows you to configure bandwidth as a percentage within low latency queueing (LLQ). Specifically, you can designate a percentage of the bandwidth to be allocated to an entity (such as a physical interface, a shaped ATM permanent virtual circuit (PVC), or a shaped Frame Relay PVC) to which a policy map is attached. Traffic associated with the policy map will then be given priority treatment. This feature also allows you to specify the percentage of bandwidth to be allocated to nonpriority traffic classes.

This feature modifies two existing commands—**bandwidth** and **priority**. This feature adds a new keyword to the **bandwidth** command—**remaining percent**. The feature also changes the functionality of the existing **percent** keyword. These changes result in the following commands for bandwidth: **bandwidth percent** and **bandwidth remaining percent.** The **bandwidth percent** command configures bandwidth as an absolute percentage of the total bandwidth on the interface. The **bandwidth remaining percent** command allows you to allocate bandwidth as a relative percentage of the total bandwidth available on the interface. This command allows you to specify the relative percentage of the bandwidth to be allocated to the classes of traffic.

This feature also adds the **percent** keyword to the **priority** command. The **priority percent** command indicates that the bandwidth will be allocated as a percentage of the total bandwidth of the interface. You can then specify the percentage (that is, a number from 1 to 100) to be allocated by using the *percentage* argument with the **priority percent** command.

Unlike the **bandwidth** command, the **priority** command provides a strict priority to the traffic class, which ensures low latency to high priority traffic classes. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftllqpct.htm.

Note This feature was originally introduced in Cisco IOS Release 12.0(5)T. This release is porting the feature into the Cisco AS5300 platform.

MD5 File Validation

The MD5 File Validation feature allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

To perform the MD5 integrity check, execute the verify command using the new "/md5" keyword. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /md5** command will calculate and disp the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, executing the **verify flash:c7200-is-mz.122-2.T.bin /MD5 8b5f3062c4caeccae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch.

A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Media Gateway Control Protocol-Based Fax (T.38) and Dual Tone Multifrequency (IETF RFC 2833) Relay

The MGCP-Based Fax (T.38) and DTMF (IETF RFC 2833) Relay feature adds support for fax relay and DTMF relay with MGCP. This feature provides two modes of implementation for each component: gateway (GW)-controlled mode and call agent (CA)-controlled mode. In GW-controlled mode, GWs negotiate DTMF and fax relay transmission by exchanging capability information in Session Descripti Protocol (SDP) messages. That transmission is transparent to the CA. GW-controlled mode allows use of the MGCP-Based Fax (T.38) and DTMF (IETF RFC 2833) Relay feature without upgrading the CA software to support the feature. In CA-controlled mode, CAs use MGCP messaging to instruct GWs to process fax and DTMF traffic. For MGCP T.38 Fax Relay, the CAs can also instruct GWs to revert to GW-controlled mode if the CA is unable to handle the fax control messaging traffic; for example, in overloaded or congested networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmgcpfx.htm.

Note Fax CODEC up-speeding is not supported.

Note **debug voip rtp [all |** ***named-event*****]** - Enables the new debug flag and displays reception or transmission of RTP named events is not supported on the Cisco AS5850, since the voice packets are CEF and would not be visible on the RSC card.

Note The Media Gateway Control Protocol-Based Fax (T.38) and Dual Tone Multifrequency (IETF RFC 2833) Relay feature was previously released in Cisco IOS Release 12.2(8)T on the Cisco 3600 series and Cisco MC3810. This feature has been added to the Cisco AS5300, Cisco AS5400, and Cisco AS5850 platforms in Cisco IOS Release 12.2(11)T.

MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles

The MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles feature implements the following Media Gateway Control Protocol (MGCP) protocols on the supported Cisco media gateways:

- MGCP 1.0 (RFC 2705)
- Network-based Call Signaling (NCS) 1.0, the PacketCable profile of MGCP 1.0 for residential gateways (RGWs)
- Trunking Gateway Control Protocol (TGCP) 1.0, the PacketCable profile of MGCP 1.0 for trunking gateways (TGWs)

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_24mg1.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5850 platforms.

MGCP Basic CLASS and Operator Services

The MGCP BCOS are a set of calling features, sometimes called "custom calling" features, that use MGCP to transmit voice, video, and data over the IP network. These features are usually found in circuit-based networks. MGCP BCOS brings them to the Cisco IOS gateways on packet-based networks.

The MGCP BCOS software is built on the MGCP CAS PBX and AAL2 software package, and supports MGCP 0.1 and the earlier protocol versions Simple Gateway Control Protocol (SGCP) 1.1 and 1.5.

The following MGCP BCOS features are available on Residential Gateways (RGWs) and Business Gateways (BGWs):

- Distinctive power ring
- Visual Message Waiting Indicator
- Caller ID
- Caller ID with Call Waiting
- Call Forwarding
- Ring Splash
- Distinctive Call Waiting Tone
- Message Waiting Tone

- Stutter Dial Tone
- Off-Hook Warning Tone

The following two features can be run as RGW or trunking gateway (TGW) features:

- 911 calls

  This feature is supported in SGCP mode on Cisco 3660 and Cisco AS5300 platforms and in MGCP mode on all five supported platforms.

- Three-Way Calling

  This feature is supported on the Cisco 3660 and Cisco AS5300 TGW platforms and on the Cisco MC3810 series, and Cisco 2600 RGW platforms. This feature cannot be supported on the G.728 and G.723 codecs.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcpgr.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feat into the Cisco AS5300 platform.

MGCP CAS PBX and AAL2 PVC

The MGCP CAS PBX and AAL2 PVC software package is a solutions-oriented program that focuses on several customer gateway scenarios. These scenarios require features that address residential, business, and trunking gateway needs on a variety of hardware platforms:

- Residential cable connectivity
- CAS and analog PBX connectivity
- Incoming CAS support for trunking gateways that support operator services such as busy-line verify and barge-in xGCP support of Voice over ATM Adaption Layer type 2 (VoAAL2)

To answer these needs, the MGCP CAS PBX and AAL2 PVC feature combines and expands existing feature sets on the merged Simple Gateway Control Protocol (SGCP)/MGCP software platform as follows:

- Voice over IP (VoIP) support of selected channel-associated signaling (CAS) features
- SGCP AAL2 features

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftmgcptk.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco AS5300 and Cisco 5850 platforms.

MGCP Generic Configuration Support for Call Manager (IP-PBX)

The MGCP Generic Configuration Support for Call Manager (IP-PBX) feature provides generic configuration support for Cisco IOS Media Gateway Control Protocol (MGCP) gateways with Call Manager. The gateways receive voice configuration from Call Manager by way of an eXtensible Markup Language (XML) file that is downloaded from a TFTP server.

MGCP Line Package Enhancements for Loop Current Feed Open (LCFO)

The MGCP Line Package Enhancements for Loop Current Feed Open (LFCO) feature enhances Media Gateway Control Protocol (MGCP) residential gateway capabilities to support the generation of the LFCO signal at the request of the call agent. LFCO is a new signal in the line package. This enhancement supports call flows that involve answering machines or other automated devices that act as the terminating party and will facilitate the notification of the originating party's on-hook to such devices. There is no explicit configuration required to enable this feature.

MGCP PRI Backhaul and T1-CAS Support for Call Manager (IP-PBX)

ISDN PRI backhaul provides a method for transporting complete IP telephony signaling information from an ISDN PRI interface of an MGCP voice gateway to Cisco CallManager through a highly reliable TCP connection.

This feature works by terminating all the ISDN PRI Layer 2 (Q.921) signaling functions in the Cisco IOS software on the MGCP voice gateway while, at the same time, packaging all the ISDN PRI Layer 3 (Q.931) signaling information into packets for transmission to the Cisco CallManager through an IP tunnel over a highly reliable TCP connection. This methodology ensures the integrity of the Q.931 signaling information being passed through the network for managing IP telephony devices.

A rich set of user-side and network-side ISDN PRI calling functions is supported by the ISDN PRI backhaul feature. A single TCP connection is used by the gateway to backhaul all the ISDN D channels to Cisco CallManager. The "SAP/Channel ID" parameter in the header of each message identifies individual D channels. In addition to carrying the backhaul traffic, the inherent TCP keepalive mechanism is also used to determine MGCP voice gateway connectivity to an available call agent.

The MGCP voice gateway also establishes a TCP link to the backup (secondary) Cisco CallManager server. In the event of Cisco CallManager switchover, the ISDN PRI backhaul functions are assumed by the secondary Cisco CallManager server. During this switchover, all active ISDN PRI calls are preserved, and the affected MGCP gateway is registered with the new Cisco CallManager server through a Restart-in-Progress (RSIP) message to ensure continued gateway operation.

T1 CAS is supported in non-backhaul fashion and supported CAS signaling types on the Cisco CallManager are E&M, wink-start, and E&M delay-dial. E1 CAS is not supported.

MGCP Voice on Cisco AS5850 Universal Gateway

Although the documents listed below were not written specifically for the Cisco AS5850, they still apply to the Cisco AS5850. MGCP Voice on Cisco AS5850 Universal Gateway include the following features:

FGD-OS 911 Calls

The 911 feature can be run as residential gateway (RGW) or trunking gateway (TGW) feature

Interactive Voice Response Version 2.0 on Cisco VoIP Gateway

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dt_skyn.htm.

Note The Configuring IVR on the Inbound VoIP Dial Peer feature and the IVR Prompts Played on IP Call Legs feature is not supported.

Media Gateway Control Protocol Residential Gateway Support

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/mgcp1213.htm

MGCP based Fax (T.38) and DTMF (IETF Ver.) Relay

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmgcpfx.htm

Note Fax CODEC up-speeding is not supported.

Note **debug voip rtp** [**all** | *named-event*] - Enables the new debug flag and displays reception.or transmission of RTP named events is not supported on the Cisco AS5850, since the voice packets are CEF and would not be visible on the RSC card.

MGCP VoIP Call Admission Control

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_04mac.htm

Network Access Server Package for Media Gateway Control Protocol

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_mgnas.htm

PRI/Q.931 Signaling Backhaul for Call Agent Applications

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/5300/sw_conf/ios_121/0144cors.htm

Route-Switch-Controller Handover Redundancy on the Cisco AS5850

See the "Route Switch Controller (RSC) Handover Redundancy" section on page 282 or refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/handred.htm

Note Route-Switch-Controller Handover Redundancy on the Cisco AS5850 features are not supported on the Cisco BTS 10200.

MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles

Refer to the following document for information:

http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_24mgl.htm

MGCP CAS PBX and AAL2 PVC

Refer to the following document for information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ftmgcpba.htm.

Further Documentation

Refer to the following document for further information about the MGCP Voice on Cisco AS5850 Universal Gateway feature:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/pull_daz.htm

MGCP VoIP Call Admission Control

MGCP VoIP Call Admission Control (CAC) determines if calls can be accepted on the IP network on the basis of available network resources. Before this release, Media Gateway Control Protocol (MGCP) Voice over IP (VoIP) calls were established regardless of the available resources on the gateway or network. The gateway had no mechanism for gracefully refusing calls if resources were not available to process the call. New calls would fail with unexpected behavior and in-progress calls would experience quality-related problems.

The MGCP VoIP Call Admission Control feature provides three CAC mechanisms to address the need for improved quality and predictable gateway behavior. The first mechanism is local/system CAC, which provides the ability to gracefully refuse calls on the basis of the availability of local gateway call processing resources such as CPU utilization and memory. The second CAC mechanism provides synchronization with Resource Reservation Protocol (RSVP) and reports the reservation request to the call agent. The third mechanism provides network congestion detection to gracefully refuse calls on the basis of a measured level of congestion.

Modem Relay Support on VoIP Platforms

When service providers and aggregators are implementing Voice over IP (VoIP), they sometimes cannot separate fax or data traffic from voice traffic. These carriers that aggregate voice traffic over VoIP infrastructures require service offerings to carry fax and data as easily as voice.

Modem relay demodulates a modem signal at one voice gateway by decomposing the modem signal to digital form and then passing this signal as packet data to another voice gateway, where the signal is remodulated and sent to a receiving modem. The relay process distinguishes that the call is in fact a modem call. On detection of the modem answer tone, the gateways switch into modem pass-through mode. If the CM (call menu) signal is detected, the two gateways switch into modem relay mode.

There are two ways to transport modem traffic over VoIP networks:

- With modem pass-through, the modem traffic is carried between the two gateways in Real-Time Transport Protocol (RTP) packets, using an uncompressed voice codec—G.711 u-law or a-law. Packet redundancy may be used to mitigate the effects of packet loss in the IP network. Even so, modem pass-through remains susceptible to packet loss, jitter, and latency in the IP network.
- With modem relay, the modem signals are demodulated at one gateway, converted to digital form, and carried in Simple Packet Relay Transport (SPRT) protocol (which is a protocol running over User Datagram Protocol [UDP]) packets to the other gateway, where the modem signal is recreated and remodulated, and passed to the receiving modem.

  In this implementation, the call starts out as a voice call and then switches into modem pass-through mode and then into modem relay mode.

This feature significantly reduces the effects that dropped packets, latency, and jitter have on the modem session. Compared to modem pass-through, it also reduces the amount of bandwidth used. Primary applications for this feature are transport of modem dial-up traffic over IP networks.

Note This version of modem relay is being made available before the ITU agrees on a standard implementation for this feature. This version of the modem relay feature will not interoperate with future versions based on the ITU implementation. When the standard ITU-based modem relay feature becomes available, the modem pass-through feature can be used for interoperability between pre-standard and standards-based modem relay platforms.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftmodrly.htm

Modem Script and System Script Support in Large-Scale Dial-Out

Modem connection and system login chat scripts are often used when asynchronous dial-on-demand routing (DDR) is configured. Currently, however, the large-scale dial-out network architecture does not allow chat scripts for a particular session to be passed through the network. Cisco IOS Release 12.2(2)T allows modem and system chat scripts to pass through large-scale dial-out networks by allocating two new authentication, authorization, and accounting (AAA) attributes for outbound service.

The AAA attributes define specific AAA elements in a user profile. Large-scale dial-out supports Cisco attribute-value (AV) pairs and TACACS+ attributes. The Modem Script and System Script Support in Large-Scale Dial-Out feature provides two new outbound service attributes for passing chat scripts: modem-script and system-script. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftlschat.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco AS5300 and Cisco AS5800 platforms.

Monitoring Voice and Fax Services on the Cisco AS5350 and Cisco AS5400 Universal Gateways

The Universal Port Dial Feature Card (DFC) is a hardware card that processes voice and data services port technology for the Cisco AS5350 and Cisco AS5400.

The ports on the Universal Port DFC support multiple types of service including modem, digital, voice and fax. Ports can be aggregated at the slot level of the Universal Port module, the Service Processing Element (SPE) level within the Universal Port module, and the individual port level.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xm/121xm_5/ftupspe.htm.

MPLS Label Distribution Protocol (LDP)

Cisco MPLS label distribution protocol (LDP) allows the construction of highly scalable and flexible IP Virtual Private Networks (VPNs) that support multiple levels of services.

LDP provides a standard methodology for hop-by-hop distribution of labels in an Multiprotocol Label Switching (MPLS) network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting label switch paths (LSPs) forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement Cisco MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_ldp7t.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5350 platform.

MPLS VPN ID

Using Multiprotocol Label Switching (MPLS) VPN ID you can identify virtual private networks (VPNs) by a VPN identification number, as described in RFC 2685. This implementation of the MPLS VPN ID feature is used for identifying a VPN. The MPLS VPN ID feature is not used to control the distribution of routing information or to associate IP addresses with MPLS VPN ID numbers in routing updates.

Multiple VPNs can be configured in a router. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the router. Alternately, you can use a VPN ID to identify a particular VPN in the router. The VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the routers in the service provider network that services that VPN.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftvpnid.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5400 platform.

Multicast Music on Hold Support for Call Manager (IP-PBX)

The Multicast Music on Hold Support for Call Manager (IP-PBX) feature provides the functionality to stream music from a Multicast Music on Hold (MOH) server to the voice interfaces of on-net and off-net callers that have been placed on hold.

This integrated multicast capability of Cisco CallManager 3.1 is implemented through the H.323 signaling plane in Cisco CallManager.

In an MOH environment, whenever caller A places caller B on hold, Cisco CallManager requests the MOH server to stream RTP packets to the "on-hold" interface through the preconfigured multicast address. In this way, RTP packets can be relayed to appropriately configured voice interfaces in a VoIP network that have been placed on hold.

Multiple MOH servers can be present in the same network, but each server must have a different Class D IP address, and the address must be preconfigured in Cisco CallManager and the Cisco IOS MGCP voice gateways.

The MOH feature enables you to subscribe to a music streaming service when using a Cisco IOS MGCP voice gateway. By means of a preconfigured multicast address on a gateway, the gateway can "listen for" Real-Time Transport Protocol (RTP) packets that are broadcast from a default router in the network and can relay the packets to designated voice interfaces in the network.

RTP is the Internet-standard protocol for transporting real-time data across a network, including audio and video information. Thus, RTP is well suited for media on demand and interactive services, such as IP telephony.

The default router in the network for handling multicast traffic must have the following enabled:

- Multicast routing
- A multicast routing protocol, for example Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP)
- An IP routing protocol, for example Routing Information Protocol (RIP) or Open Shortest Path First (OSPF)

When you configure a multicast address on a gateway, the gateway sends an Internet Gateway Management Protocol (IGMP) "join" message to the default router, indicating to the default router that the gateway is to receive RTP multicast packets.

Multiple RSA Keypair Support

The Multiple RSA Keypair Support feature allows the Cisco IOS software to maintain a distinct key for each certification authority (CA) with which it is dealing. Thus, the Cisco IOS software can match policy requirements for each CA without compromising the requirements specified by the other CAs, such as key length, key lifetime, and general-purpose versus special-usage keys.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmltkey.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

NAT Support for SIP

The Session Initiation Protocol (SIP) is an application layer signaling protocol used for creating and controlling multimedia sessions with two or more participants. SIP is transported over TCP or UDP. The messages used in the protocol may have IP addresses embedded in the packet payload. If a message passes through a router configured with Network Address Translation (NAT), the embedded information must be translated and encoded back to the packet. An Application Layer Gateway (ALG) is used with NAT to enable SIP.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftnatsip.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

NetFlow Multiple Export Destinations

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to the destination host. Currently, the maximum number of export destinations allowed is two.

The NetFlow Multiple Export Destinations feature improves the chances of receiving complete NetFlow data by providing redundant streams of data. Because the same export data is sent to more than one NetFlow collector, fewer packets will be lost. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/dtnfdest.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300 and Cisco AS5800 platforms.

NetFlow ToS-Based Router Aggregation

The NetFlow ToS-Based Router Aggregation feature provides the ability to enable limited router-based type of service (ToS) aggregation of NetFlow Export data, which results in summarized NetFlow Export data to be exported to a collection device. The result is lower bandwidth requirements for NetFlow Export data and reduced platform requirements for NetFlow data collection devices. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s15/dtnfltos.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300 and Cisco AS5800 platforms.

Network Access Server (NAS) Package for MGCP

The Network Access Server (NAS) Package for MGCP feature adds support for the Media Gateway Control Protocol (MGCP) NAS package on the Cisco AS5350, Cisco AS5400, and Cisco AS5850. With this implementation, data calls can be terminated on a trunking media gateway that is serving as a NAS. Trunks on the NAS are controlled and managed by a call agent that supports MGCP for both voice and data calls. The call agent must support the MGCP NAS package.

These capabilities are enabled by the universal port functionality of the Cisco AS5350, Cisco AS5400, and Cisco AS5850, which allows these platforms to operate simultaneously as network access servers and voice gateways to deliver universal services on any port at any time. These universal services include dial access, real-time voice and fax, wireless data access, and unified communications.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_mgnas.htm.

Network Side ISDN PRI Signaling, Trunking, and Switching

The Network Side ISDN PRI Signaling, Trunking, and Switching feature enables Cisco IOS software to replicate the public switched network interface to a PBX that is compatible with the National ISDN (NI) switch types and European Telecommunications Standards Institute (ETSI) Net5 switch types.

Routers and PBXs are both traditionally CPE devices with respect to the public switched network interfaces. However, for Voice over IP (VoIP) applications, it is desirable to interface access servers to PBXs with the access server representing the public switched network.

Enterprise organizations use the current VoIP features with Cisco products as a method to reduce costs for long distance phone calls within and outside their organizations. However, there are times that a call cannot go over VoIP and the call needs to be placed using the Public Switched Telephone Network (PSTN). The customer then must have two devices connected to a PBX to allow some calls to be placed using VoIP and some calls to be placed over the PSTN. In contrast, this feature allows Cisco access servers to connect directly to user-side CPE devices such as PBXs and allows voice calls and data calls to be placed without requiring two different devices to be connected to the PBXs.

The ISDN Network Side ISDN PRI Signaling, Trunking, and Switching feature allows Cisco ISDN-enabled access servers to switch calls across interfaces as legacy phone switches do today and to mimic the behavior of the legacy phone switches.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtpri_ni.htm.

Nonblocking Gatekeeper AAA Interface

The Nonblocking Gatekeeper AAA Interface feature enables Cisco gatekeepers to perform authentication, authorization, and accounting (AAA) through the gatekeeper interface at much high call rates.

There are no new or modified commands.

Optimized PPP Negotiation

The Optimized PPP Negotiation feature optimizes the time needed for PPP negotiation when a connection is made. PPP negotiation can include several cycles before the negotiation options are acknowledged. These negotiation cycles can cause a significant user-perceived delay, especially in networks with slow links such as a wireless data connection. Additionally, the PPP negotiation time can add significantly to the total time the user stays connected in these types of connections. Changes to the PPP link control protocol (LCP) and PPP Internet Protocol Control Protocol (IPCP) negotiation strategies as part of Cisco IOS Release 12.2(4)T and later releases make a reduction in the negotiation time possible.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftcphneg.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300 and Cisco AS5800 platforms.

OSP Debug Enhancement

The OSP Debug Enhancement feature documents the new **debug voip settlement ssl** command. Use this command if you find a connection or I/O error with the Secure Socket Layer (SSL) connection after using the **debug voip settlement error** command. Turning on the **debug voip settlement ssl** command allows the Open Settlement Protocol (OSP) to display detailed information for the SSL connection.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftdbgosp.htm

OSPF ABR Type 3 LSA Filtering

The OSPF ABR Type 3 link-state advertisement (LSA) Filtering feature extends the ability of an ABR that is running the OSPF protocol to filter type 3 LSAs between different OSPF areas. This feature allows only specified prefixes to be sent from one area to another area and restricts all other prefixes. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11at3f.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

OSPF Sham-Link Support for MPLS VPN

A sham link is a logical path within an Open Shortest Path First (OSPF) area; it represents an unnumbered point-to-point connection between two provider edge (PE) devices. All routers within the area see the link and use it during the shortest path first (SPF) computation.

On PE routers the VPN Route Forwarding (VRF) routing table is populated by OSPF routes over the sham link. The sham link gives users the capability of specifying which path will be used for traffic.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ospfshmk.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

OSPF Stub Router Advertisement

The OSPF Stub Router Advertisement feature allows you to bring a new router into a network without immediately routing traffic through the new router and allows you to gracefully shut down or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration options that allow you to configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum or infinite metric to all neighbors. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11osra.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

OSPF Update Packet-Pacing Configurable Timers

The OSPF Update Packet-Pacing Configurable Timers feature allows you to configure the rate at which Open Shortest Path First (OSPF) link-state advertisement (LSA) flood pacing, group pacing, and retransmission pacing updates occur. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft11opct.htm

.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300 platform.

Particle Drivers

The Particle Drivers feature is a collection of performance and reliability improvements for the Cisco AS5350, Cisco AS5400, and Cisco AS5400HPX universal gateways. It includes particles-based packet drivers for improved performance. These particle drivers optimize Cisco IOS fast switching code and significantly improve the way Cisco IOS uses processor cache memory. Data packets for some protocols, such as MLPPP, IP Multicast, and cRTP, are fast switched with particle drivers. Cisco IOS CEF switching paths are highly optimized with particle drivers.

PIAFS Wireless Data Protocol Version 2.1 for Cisco MICA Modems

The PIAFS Wireless Data Protocol Version 2.1 for Cisco MICA Modems feature adds support for the Personal Handyphone Internet Access Forum Standard (PIAFS) using Cisco MICA technologies modems for the Cisco AS5300 and Cisco AS5800. PIAFS provides data connectivity between a client computer and a remote access server (RAS) using the Personal-Handyphone-System (PHS) digital cellular telephone system. PIAFS 2.1 allows the modem to shift speed during a connection between 32,000 and 64,000 bps when initiated by a remote terminal adapter (TA).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftblknt.htm.

PIM Multicast Scalability

The PIM Multicast Scalability feature enhances the Protocol Independent Multicast (PIM) protocol in Cisco IOS software by adding a new level of scalability. With this feature, edge devices can have a large number of multicast groups and users without increasing the CPU utilization of the router.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

PIM MIB Extension for IP Multicast

Protocol Independent Multicast (PIM) is an IP Multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the *Protocol Independent Multicast for IPv4* MIB, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).

The PIM MIB Extension for IP Multicast feature introduces support in Cisco IOS software for the CISCO-PIM-MIB, which is an extension of RFC 2934 and an enhancement to the existing Cisco implementation of the PIM MIB.

This feature introduces the following new classes of PIM notifications:

- neighbor-change—This notification results from the following conditions:
  - When the PIM interface of a router is disabled or enabled (using the **ip pim** command in interface configuration mode)
  - When the PIM neighbor adjacency of a router expires or is established (defined in RFC 2934)
- rp-mapping-change—This notification results from a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
- invalid-pim-message—This notification results from the following conditions:
  - When an invalid (*, G) join or prune message is received by the device (for example, when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group)
  - When an invalid PIM register message is received by the device (for example, when a router receives a register message from a multicast group for which it is not the RP)

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftpimmib.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Preauthentication with ISDN PRI and Channel-Associated Signalling Enhancements

Preauthentication allows a Cisco network access server (NAS) to decide—on the basis of the Dialed Number Identification Service (DNIS) number—whether to answer an incoming call. When an incoming call arrives from the public network switch but before it is answered, the NAS sends the DNIS number to a RADIUS server for authorization.

The Preauthentication with ISDN PRI and Channel-Associated Signaling Enhancements feature provides additional support for preauthentication, which was introduced in a previous Cisco IOS release. For more information about preauthentication, refer to the Cisco IOS Release 12.1(3)T feature module titled *Preauthentication with ISDN PRI and Channel-Associated Signaling*.

This feature supports the use of attribute 44 by the RADIUS server application, which allows user authentication on the basis of the Calling Line Identification (CLID) number in the same transaction. For more information about attribute 44 and how it works with preauthentication, refer to the Cisco IOS Release 12.0(7)T feature module titled *RADIUS Attribute 44 (Accounting Session ID) in Access Requests*.

This feature also supports the use of new RADIUS attributes. These RADIUS attributes are configured in the RADIUS preauthentication profiles to specify preauthentication behavior. They may also be used, for instance, to specify whether subsequent authentication should occur and, if so, what authentication method should be used. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdt1.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(5)T. This release is porting the feature into the Cisco AS5350 and Cisco AS5850 platforms.

PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer

The PRI Backhaul Using the Stream Control Transmission Protocol and the ISDN Q.921 User Adaptation Layer feature fulfills the need for a standards-based PRI signaling backhaul that works with third-party call agents to enable solutions like Integrated Access, IP PBX, and Telecommuter.

This feature provides the following:

- PRI backhaul—Specific implementation for backhauling PRI.
- Stream control transmission protocol (SCTP)—New general transport protocol that can be used for backhauling signaling messages.
- ISDN Q.921 User Adaptation Layer (IUA)—Mechanism for backhauling any Layer 3 protocol that normally uses Q.921.

This feature provides a configuration interface for Cisco IOS software implementation and implements the protocol message flows for SCTP and IUA.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ft_0546.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5850 platform.

PRI/Q.931 Signaling Backhaul for Call Agent Applications

The PRI/Q.931 Signaling Backhaul for Call Agent Applications feature implements PRI/Q.931 signaling backhaul support for call agent applications on the Cisco 2600 and Cisco 3600 series routers and Cisco MC3810 series access concentrators. PRI/Q.931 signaling backhaul is the transport of PRI signaling (Q.931 and above layers) between a media gateway (such as a Cisco access server, router, or concentrator) and a media gateway controller (Cisco VSC3000).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/as5400/sw_conf/ios_122/122_2x/122xb/pul0144.htm.

Note This feature was originally introduced in Cisco IOS Release 12.1(1)T on the Cisco AS5300 platform This release is porting the feature into the Cisco AS5350, CIsco AS5400, and Cisco AS5850 platform.

PSTN Fallback

The goal of PSTN fallback is to monitor congestion in the IP network and either redirect calls to the PSTN or reject calls based on the network congestion. Calls can be rerouted to an alternate IP destination or to the PSTN if the IP network is found unsuitable for voice traffic at that time. The user defines the congestion thresholds based on the configured network. This functionality enables the service provider to give a reasonable guarantee about the quality of the conversation to their VoIP users at the time of call admission.

Note PSTN fallback does not provide assurances that a VoIP call that proceeds over the IP network is protected from the effects of congestion. This is the function of the other Quality of Service (QoS) mechanisms such as IP Real-Time Transport Protocol (RTP) priority or low latency queuing (LLQ).

PSTN fallback includes the following features:

- Offers flexibility to define the congestion thresholds based on the network.
  - Defines a threshold based on Calculated Planning Impairment Factor (ICPIF), which is derived as part of International Telecommunication Union (ITU) G.113.
  - Defines a threshold based solely on packet delay and loss measurements.
- Uses Service Assurance Agent (SAA) probes to provide packet delay, jitter, and loss information for the relevant IP addresses. Based on the packet loss, delay, and jitter encountered by these probes, an ICPIF or delay and loss values are calculated.
- Is supported by calls of any codec. Only G.729 and G.711 have accurately simulated probes. Calls of all other codecs are emulated by a G.711 probe.

For more information, including configuration tasks and examples, and command references for PSTN fallback, please refer to PSTN Fallback. Refer to the following document for additional information about the Call Admission Control for H.323 VoIP Gateways feature:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ft_pfavb.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

QSIG for TCL IVR 2.0

Q.SIG support is required for European countries to interconnect enterprise customers to a wholesale voice solution. The Q.SIG for TCL IVR 2.0 feature provides transparent Q.SIG interworking when using a TCL IVR version 2.0 voice application on a Cisco IOS voice gateway. This functionality can be enabled using a new CLI on the POTS or VoIP dial peer. Before this feature, Q.SIG messages were interpreted by the TCL IVR 2.0 application, rather than passed transparently to the remote endpoint.

R2 and ISUP Transparency and R2-to-ISUP Interworking Enhancements

The R2 and ISUP Transparency and R2-to-ISUP Interworking Enhancements feature provides enhancements to ISDN User Part (ISUP) transparency, R2-to-ISUP interworking, and R2 transparency using Generic Transparency Descriptor (GTD) objects in Cisco IOS Release 12.2(11)T. This release also provides support for Calling Line ID Presentation (CLIP) and Calling Line ID Restriction (CLIR) and is part of the Cisco SS7 Interconnect for Voice Gateways Solution.

This feature adds the following functionality:

- Additional platform support for Cisco AS5800, Cisco AS5850, Cisco 3660, and Cisco 7200 series routers.
- CLIP and CLIR interworking between ISUP and H.225.
- Global Call Correlation ID GTD parameter generation.

- Global Call Correlation ID GTD parameter relay through the originating and terminating gateways between the Cisco SC2200 NI2+ and H.323 interfaces.
- Nonstandard CPC values support using FDC.
- R2-to-ISUP delayed release interworking using GTD.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_isup1.htm.

RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements

Virtual private networks (VPNs) use Layer 2 Forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP) tunnels to tunnel the link layer of high-level protocols (for example, PPP) or asynchronous High-Level Data Link Control (HDLC)). Internet service providers (ISPs) configure their network access servers (NASs) to receive calls from users and forward the calls to the customer tunnel server. Usually, the ISP maintains only information about the tunnel server—the tunnel endpoint. The customer maintains the IP addresses, routing, and other user database functions of the tunnel server users.

The RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements feature adds the ability to specify the host name of the NAS—rather than the IP address of the NAS—in RADIUS attribute 66 (Tunnel-Client-Endpoint). Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dtdt4.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

RADIUS Attribute 82: Tunnel Assignment ID

The RADIUS Attribute 82: Tunnel Assignment ID feature allows the Layer 2 Transport Protocol access concentrator (LAC) to group users from different per-user or domain RADIUS profiles into the same active tunnel. Previously, Cisco IOS software assigned a separate virtual private dialup network (VPDN) tunnel for each per-user or domain RADIUS profile, even if tunnels with identical endpoints already existed. The RADIUS Attribute 82: Tunnel Assignment ID feature defines a new AV pair, Tunnel-Assignment-ID, which allows the LAC to group users from different RADIUS profiles into the same tunnel if the chosen endpoint, tunnel type, and Tunnel-Assignment-ID are identical. This feature introduces new software functionality. No new commands are introduced with this feature.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftrada82.htm
.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release ports the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

RADIUS Attribute Value Screening

The RADIUS Attribute Value Screening feature allows users to configure a list of "accept" or "reject" RADIUS attributes on the network access server (NAS) for purposes such as authorization or accounting.

If a NAS accepts and processes all RADIUS attributes received in an Access-Accept packet, unwanted attributes may be processed, creating a problem for wholesale providers who do not control their customers' authentication, authorization, and accounting (AAA) servers. For example, there may be attributes that specify services to which the customer has not subscribed, or there may be attributes that may degrade service for other wholesale dial users. The ability to configure the NAS to restrict the use of specific attributes has therefore become a requirement for many users.

The RADIUS Attribute Value Screening feature should be implemented in one of the following ways:

- To allow the NAS to accept and process all standard RADIUS attributes for a particular purpose, except for those on a configured reject list.
- To allow the NAS to reject (filter out) all standard RADIUS attributes for a particular purpose, except for those on a configured accept list.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T as the RADIUS Attribute Screening feature for the Cisco 7200 series router. This release ports the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

RADIUS Number Translation VSAs for VoIP

The RADIUS Number Translation VSAs for VoIP feature enables a Cisco AS5x00 voice gateway to export pre- and post-translated called and calling numbers to a RADIUS server in the form of generic vendor-specific attributes (VSA). Cisco gateways can be configured to present gateway received, gatekeeper translated, and final translated numbers to the RADIUS server.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/vsaig3.htm.

RADIUS Packet of Disconnect

The RADIUS Packet of Disconnect feature consists of a method for terminating a call that has already been connected. This "Packet of Disconnect" (POD) is a RADIUS access_request packet and is intended to be used when the authenticating agent server wants to disconnect the user after the session has been accepted by the RADIUS access_accept packet. This may be needed in at least two situations:

- Detection of fraudulent use, which cannot be performed before accepting the call. A price structure so complex that the maximum session duration cannot be estimated before accepting the call. This may be the case when certain types of discounts are applied or when multiple users use the same subscription simultaneously.
- To prevent unauthorized servers from disconnecting users, the authorizing agent that issues the POD packet must include three parameters in its packet of disconnect request. For a call to be disconnected, all parameters must match their expected values at the gateway. If the parameters do not match, the gateway discards the packet of disconnect packet and sends a NACK (negative acknowledgement message) to the agent.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_pod1.htm.

RADIUS Packet Suppression for VoIP GW Rotary Dial-Peer Attempts

The RADIUS Packet Suppression for VoIP GW Rotary Dial-Peer Attempts feature enables the suppression of excess RADIUS start and stop requests that are sent when the originating or terminating gateway does rotary dial-peer retries for outbound call legs. When the rotary retry suppression feature is enabled, only one set of start and stop accounting packets is generated once a connection is successful or once the connection fails in the last rotary dial-peer attempt.

The rotary retry suppression feature gives you more control over authentication, authorization, and accounting (AAA) functions by enabling or disabling accounting on outgoing call legs. Standard RADIUS accounting enabled on the voice gateway sends a start and stop accounting request to RADIUS on every attempt using a rotary dial peer for making a connection. Every attempt can generate a pair of accounting requests even when the connection is not successful. The rotary retry suppression feature eliminates unnecessary traffic flow to the RADIUS server or other Voice over IP (VoIP) billing servers. When the rotary retry feature is activated, no matter how many dial peers are used for the outgoing call leg, only one pair of accounting start and stop records is sent to the billing server.

There is one modified command: **suppress rotary**—the keyword, **rotary**, was added to enable rotary retry suppression.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftsuppre.htm.

RADIUS Preauthentication for H.323 and SIP Voice Calls

The RADIUS Preauthentication for H.323 and SIP Voice Calls feature provides the means for service providers to accept or reject H.323 or SIP voice calls that come in to their networks before the calls are answered. This feature allows a wholesale service provider to screen an originating (PSTN-to-IP network) or terminating (IP-to-PSTN) voice call by using information about the call to determine which customer the call belongs to and whether the call should be admitted to the network. The type of information that can be used for screening includes the called number, the called number prefix, the originating H.323 zone and the originating voice gateway address. The service provider can use this feature in conjunction with a RADIUS-based port-policy management (PPM) server such as Cisco Resource Policy Management Server (RPMS) to make admission control decisions on the basis of information such as the total number of calls in the network, the total number of calls allowed for this customer and the current number of calls from this customer.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_trg.htm.

RADIUS Progress Codes

The RADIUS Progress Codes feature adds additional progress codes—10, 31, 32, 60, 65, 67—to RADIUS attribute 196 (Ascend-Connect-Progress), which indicates the connection state before the call is disconnected via progress codes.

Attribute 196 is sent in network, exec, and resource accounting start and stop records. This attribute can facilitate call failure debugging because each progress code identifies accounting information relevant start or stop record is requested, authentication, authorization, and accounting (AAA) will add attribute 196 into the record as part of the standard attribute list.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftatr196.htm.

RADIUS Route Download

The RADIUS Route Download feature allows users to configure their network access server (NAS) to send static route download requests to authentication, authorization, and accounting (AAA) servers specified by a named method list. Before this feature, all RADIUS authorization requests for static route download could be sent only to AAA servers specified by the default method list.

This feature extends the functionality of the **aaa route download** command to allow users to specify the name of the method list that will be used to direct static route download requests to the AAA servers. The **aaa route download** command must be used to add separate method lists; however, users will continue to enable the **aaa authorization configuration default** command to download static route configuration information from the AAA server specified by the default method list.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftradrou.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

RADIUS Tunnel Preference for Load Balancing and Fail-over

Tunnel servers may be load balanced or failed-over from a single tunnel initiator, as selected by the RADIUS Tunnel Preference for Load Balancing and Fail-Over attribute. There is no configuration associated with this feature. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftradtun.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release ports the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Reverse Path Forwarding - Source Exists Only

The Reverse Path Forwarding - Source Exists Only feature allows you to verify if the source IP address is valid in the Forwarding Information Base (FIB) for unicast Reverse Path Forwarding (uRPF) traffic. Packets that have not be allocated on the Internet, being used for spoofed source addresses, will be dropped. Packets with an entry in the FIB will be passed. This uRPF option can be used on internet service provider (ISP) peering routing devices with other ISPs.

Rotating Through Dial Strings

The Rotating Through Dial Strings feature allows you to specify the dialing order when multiple dial strings are configured. Options for dialing order include:

- Sequential—Dial using the first dial string configured in a list of multiple strings.
- Round-robin—Dial using the dial string following the most recently successful dial string.
- Last successful call—Dial using the most recently successful dial string.

This feature takes advantage of information available from a previous call attempt, such as whether the call was unsuccessful or the line was busy, and thereby increases the rate of successful calls.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftrotdls.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Route Switch Controller (RSC) Handover Redundancy

Route-Switch-Controller Handover Redundancy on the Cisco AS5850, with its provision of handover-split mode, provides the first phase of high availability to the Cisco AS5850 platform.

If your gateway contains two route-switch-controller (RSC) cards, you can configure your Cisco AS5850 into either of two split modes: classic split or handover split.

Note Route-Switch-Controller Handover Redundancy on the Cisco AS5850 features are not supported on the Cisco BTS 10200.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/handred.htm.

Router-Shelf Redundancy for the AS5800 Series

This feature provides AS5800 router-shelf redundancy by using a second router shelf that automatically takes over the other shelf's resources (dial-shelf cards) if it appears that the other router has died. The failover is disruptive in that there is no attempt to maintain calls that were established on the failing router; the dial-shelf cards controlled by the failing router are restarted under the control of the backup router and hence become available again.

Two router shelves are connected to the same dial shelf (as in split mode) but with only one router active at a time. Both router shelves are configured for normal mode as opposed to split mode. Each router shelf contains the same configuration, being whatever configuration is appropriate for the full set of cards in the dial shelf. The active router controls all the cards in the dial shelf, while the other router functions purely as a backup. If the active router fails, all dial-shelf cards restart under the control of the backup router, which then functions as the active router.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121x/121xv/121xv_5/ftred3.htm.

SGCP RSIP and AUEP Enhancement

The SGCP RSIP and AUEP Enhancement feature provides additional messaging capabilities that allow an endpoint on an SGCP 1.5 gateway to synchronize with a call agent after the endpoint returns to service from the disconnected procedure. The additional messaging capabilities provide the following:

- A special disconnected-RSIP message that the gateway sends to the call agent as a result of the disconnected procedure.
- Additional fields in the AUEP command that the call agent uses to query the endpoint's status when contact is reestablished.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_rsip.htm.

Shell-Based Authentication of VPDN Users

The Shell-Based Authentication of VPDN Users feature provides terminal services for VPDN users to support rollout of wholesale dial networks. Terminal services (shell login or exec login) on the network access server (NAS) provide the following capabilities:

- Enabling a dial-in user session to be terminated at the access server.
- Authenticating the user with a character-mode login dialog such as username/password or username/challenge/password, Secure ID, Safeword, and so on.
- Initiating PPP and tunneling it to a home gateway (HGW).

With the terminal services, user authentication methods other than PAP and CHAP can be applied to PPP users. With the Shell-Based Authentication of VPDN Users feature, PPP authentication data is preconfigured or entered before PPP starts. Authentication is completed without any further input from the user. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122defer/ftexvpnt.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release ports the feature into the Cisco AS5300 and Cisco AS5800 platforms.

SIP—Call Transfer Using Refer Method

Note The SIP—Call Transfer Using Refer Method feature is also known under the feature title Call Transfer Capabilities Using the Refer Method.

The Refer method provides call transfer capabilities to supplement the Bye and Also methods already implemented on Cisco IOS Session Initiation Protocol (SIP) gateways.

Call transfer allows a wide variety of decentralized multiparty call operations. These decentralized call operations form the basis for third-party call control and thus are important features for Voice over IP (VoIP) and SIP. Call transfer is also critical for conference calling, where calls can transition smoothly between multiple point-to-point links and IP level multicasting.

The following are components of call transfer:

- Refer Method
- Refer-To Header
- Referred-By Header
- Notify Method
- Using the Refer Method to Achieve Call TransferBlind Transfer
- Attended Transfer

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftrefer.htm.

Note This feature was previously released in Cisco IOS Release 12.2(8)T for the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

SIP Carrier Identification Code

The SIP Carrier Identification Code feature enables the transmission of the Carrier Identification Code (CIC) parameter from the Session Initiation Protocol (SIP) network to the ISDN. The CIC parameter is a three- or four- digit code that is used in routing tables to identify the network serving the remote user when a call is routed over many different networks. The CIC parameter is carried in SIP INVITE requests and 302 REDIRECTs and maps to the ISDN Transit Network Selection Information Element (TNS IE) in the outgoing ISDN SETUP message. The TNS IE identifies the requested transportation networks and allows different providers equal access support based on customer choice.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftsipcic.htm.

SIP—Configurable PSTN Cause Code Mapping

For calls to be established between a session initiation protocol (SIP) network and a PSTN network, the two networks must be able to interoperate. One aspect of their interoperation is the mapping of PSTN cause codes, which indicate reasons for Public Switched Telephone Network (PSTN) call failure or completion, for SIP status codes or events. The opposite is also true: SIP status codes or events are mapped to PSTN cause codes. Event mapping tables found in this document show the standard or default mappings between SIP and PSTN.

However, you may want to customize the SIP user agent software to override the default mappings between the SIP and PSTN networks. The Configurable PSTN Cause Code to SIP Response Mapping feature allows you to configure specific map settings between the PSTN and SIP networks. Thus, any SIP status code can be mapped to any PSTN cause code, or vice versa. When set, these settings can be stored in the NVRAM and are restored automatically on bootup.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmap.htm.

Note This feature was previously released in Cisco IOS Release 12.2(8)T for the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers as Configurable PSTN Cause Code to SIP Response Mapping. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 platforms.

SIP—DNS SRV RFC2782 Compliance

Session Initiation Protocol (SIP) on Cisco Voice over IP (VoIP) gateways uses Domain Name System Server (DNS SRV) query to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." and is attached to the fully qualified domain name (FQDN) of the next hop SIP server. This prefix style, from RFC 2052, has always been available; however, with this release, a second style is also available. The second style complies with RFC 2782 and prepends the protocol label with an underscore "_"; as in "_protocol._transport." The addition of the underscore reduces the risk of the same name being used for unrelated purposes. The form compliant with RFC 2782 is the default style. Use the **srv version** command to configure the DNS SRV feature.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/vvfresrv.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

SIP Diversion Header Implementation for Redirecting Number

SIP is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to the ITU-T H.323 specification. SIP is defined by RFC 2543 and is used for multimedia call session setup and control over IP networks. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/sipcf2.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release ports the feature into the Cisco AS5300 and Cisco AS5400 platforms.

SIP—Enhanced Billing Support for Gateways

The Enhanced Billing Support for SIP Gateways feature provides changes to authentication, authorization, and accounting (AAA) records and the RADIUS implementations on Cisco session initiation protocol (SIP) gateways. These changes were introduced to provide customers and partners the ability to effectively bill for traffic transported over SIP networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmsnbil.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T as Enhanced Billing Support for SIP Gateways. This release is porting the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

SIP Gateway Support for the Bind Command

In previous releases of Cisco IOS software, the source address of a packet going out of the gateway was never deterministic. That is, the session protocols and Voice over IP (VoIP) layers always depended on the IP layer to give the *best local address*. The best local address was then used as the source address (the address showing where the SIP request came from) for signaling and media packets. Using this nondeterministic address occasionally caused confusion for firewall applications, because a firewall could not be configured with an exact address and would take action on several different source address packets.

However, the bind interface command allows you to configure the source IP address of signaling and media packets to a specific interface's IP address. Thus, the address that goes out on the packet is bound to the IP address of the interface specified with the bind command. Packets that are not destined to the bound address are discarded.

When you do not want to specify a bind address, or if the interface is down, the IP layer still provides the best local address.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftbind.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

SIP Gateway Support for Third Party Call Control

SIP is a new protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multim Session Control (MMUSIC) Working Group as an alternative to the ITU-T H.323 specification. SII defined by RFC 2543 and is used for multimedia call session setup and control over IP networks. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/sipcf2.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release ports the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5850 platforms.

SIP Gateway Support of RSVP and TEL URL

The SIP Gateway Support of RSVP and TEL URL feature also supports Telephone Uniform Resource Locators or TEL URL. Currently session initiation protocol (SIP) gateways support URLs in the SIP format. SIP URLs are used in SIP messages to indicate the originator, recipient, and destination of the SIP request. However, SIP gateways may also encounter URLs in other formats, such as TEL URLs. TEL URLs describe voice call connections. They also enable the gateway to accept TEL calls sent through the Internet and to generate TEL URLs in the request line of outgoing INVITE requests.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/ xb_2/vvfresrv.htm.

Note This feature was previously released in Cisco IOS Release 12.2(8)T for the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

SIP INFO Method for DTMF Tone Generation

The SIP INFO Method for DTMF Tone Generation feature adds support for dual tone multifrequency (DTMF) tone generation to allow out-of-band signaling. The SIP INFO method is used to generate DTMF tones on the telephony call leg. The SIP INFO method or request message is used by a user agent

(UA) to send call signaling information to another UA with which it has an established media session. The SIP INFO message is sent along the signaling path of the call. Upon receipt of a SIP INFO message with DTMF relay content, the gateway generates the specified DTMF tone on the telephony end of the call.

The SIP INFO Method for DTMF Tone Generation feature is always enabled and is invoked when a SIP INFO message is received with DTMF relay content. This feature is related to the DTMF Events Through SIP Signaling feature, which provides the ability for an application to be notified about DTMF events using SIP NOTIFY messages. Together, the two features provide a mechanism to both send and receive DTMF digits along the signaling path.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftinfo.htm.

SIP Intra-gateway Hairpinning

SIP hairpinning is a call routing capability in which an incoming call on a specific gateway is signaled through the IP network and back out the same gateway. This call can be a public switched telephone network (PSTN) call routed into the IP network and back out to the PSTN over the same gateway.

Similarly, SIP hairpinning can be a call signaled from a line (for example, a telephone line) to the IP network and back out to a line on the same access gateway. With SIP hairpinning, unique gateways for ingress and egress are no longer necessary.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

SIP INVITE Request with Malformed Via Header

SIP INVITE requests that a user or service participate in a session. Each INVITE contains a Via header that indicates the transport path taken by the request so far and where to send a response. In the past, when an INVITE contained a malformed Via header, the gateway would print a debug message and discard the INVITE without incrementing a counter. However, the printed debug message was often inadequate, and it was difficult to detect that messages were being discarded.

The SIP INVITE Request with Malformed Via Header feature provides a response to the malformed request. A counter, Client Error: Bad Request, increments when a response is sent for a malformed Via field. Bad Request is a class 400 response and includes the explanation Malformed Via Field. The response is sent to the source IP address (the IP address where the SIP request originated) at User Datagram Protocol (UDP) port 5060.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmalvia.htm.

Note This feature was previously released in Cisco IOS Release 12.2(8)T on the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers. This release ports the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

SIP Multiple 18x Responses

The SIP Multiple 18x Responses feature enhances forking support on the user agent client (UAC) by supporting sequential forking. With sequential forking the UAC receives multiple provisional responses (18x) but treats each response as a separate call leg. This allows the proxy to initiate a new INVITE if the called party does not pick up.

SIP—Session Initiation Protocol for VoIP

Voice over IP (VoIP) currently implements the ITU H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. Session Initiation Protocol (SIP) is a protocol developed by the Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group as an alternative to H.323. The Cisco SIP functionality equips Cisco routers to signal the setup of voice and multimedia calls over IP networks. SIP provides an alternative to H.323 within the VoIP internetworking software.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_sip72.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T as Session Initiation Protocol (SIP) for VoIP. This release ports the feature into the Cisco AS5850 platform.

SIP—Session Iniation Protocol for VoIP Enhancements

Voice over IP (VoIP) currently implements the International Telecommunication Union (ITU)'s H.323 specification within Internet Telephony Gateways (ITGs) to signal voice call setup. The Session Initiation Protocol (SIP) is a new protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP. SIP features are compliant with IETF RFC 2543, *SIP: Session Initiation Protocol*, published in March 1999.

The Cisco SIP functionality, introduced in Cisco IOS Release 12.1(1)T and enhanced in Cisco IOS Release 12.1(3)T, enables Cisco access platforms to signal the setup of voice and multimedia calls over IP networks. The SIP feature also provides nonproprietary advantages in the areas of

- Protocol extensibility
- System scalability
- Personal mobility services
- Interoperability with different vendors

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftsipgv.htm.

SIP Session Timr Support

The SIP Session Timer Support feature adds the capability of a periodic refresh of session initiation protocol (SIP) sessions by sending repeated INVITE requests. The repeated INVITE requests, or re-INVITEs, are sent during an active call leg to allow user agents (UAs) or proxies to determine the status of a SIP session. Without this keepalive mechanism, proxies that remember incoming and outgoing requests (stateful proxies) may continue to retain call state needlessly. If a UA fails to send a

BYE message at the end of a session or if the BYE message gets lost because of network problems, a stateful proxy does not know that the session has ended. The re-INVITES ensure that active sessions stay active and that completed sessions are terminated.

The SIP Session Timer Support feature also adds two new general headers that are used to negotiate the value of the refresh interval.

- The Session-Expires header is used in an INVITE if the user agent client (UAC) wants to use the session timer.
- The Min-SE header conveys the minimum allowed value for the session expiration.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftsiptim.htm.

SIP T.37 Store and Forward Fax

SIP T.37 is an ITU specification that enables store-and-forward fax applications, as well as toggling from voice to fax, for example, providing an Interactive Voice Response (IVR) front end to a store-and-forward fax application.

Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/index.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

SIP T.38 Fax Relay

The SIP T.38 Fax Relay feature adds standards-based fax support to session initiation protocol (SIP) and conforms to ITU-T T.38 Procedures for real-time Group 3 facsimile communication over IP networks. The ITU-T standard specifies real-time transmission of faxes between two regular fax terminals over an IP network. Much like a voice call, SIP T.38 Fax Relay requires call establishment, data transmission, and release signaling.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftsipfax.htm.

Note This feature was previously released in Cisco IOS Release 12.2(8)T for the Cisco 2600 series and Cisco 3600 series routers. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

SIP User Agent MIB

The Session Initiation Protocol (SIP) User Agent Client (UAC) and User Agent Server (UAS) are manageable by an SNMP-based network management platform, such as the Cisco Voice Manager. The SIP UAC/UAS exists on the AS5300 and AS5400 platforms. The SIP MIB has been defined, will be submitted to the IETF, and will be implemented on those platforms.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB web site on Cisco.com at the following location:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

SNMP Support over VPN

The SNMP Support over VPN feature allows the sending and receiving of SNMP notifications using VPN Routing Forwarding table (VRF).

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents.

A VPN is a network that provides high connectivity transfers on a shared system with the same usage guidelines as a private network. A VPN can be built on the Internet or on the service provider IP, Frame Relay, or ATM system.

A VRF stores per-VPN routing data. It defines the VPN membership of a customer site attached to the network access server (NAS). A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, guidelines, and routing protocol parameters that control the information that is included in the routing table.

The SNMP Support over VPN feature provides configuration commands that allow users to associate SNMP agents and managers with specific VRFs. The specified VRF is used for the sending of SNMP notifications (traps and informs) and responses between agents and managers. If a VRF is not specified, the default routing table for the VPN is used. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftnm_vpn.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(2)T. This release ports the feature into the Cisco AS5300 and Cisco AS5800 platforms.

SNMPv3 Community MIB Support

The SNMPv3 Community MIB Support feature implements support for the SNMP Community MIB (SNMP-COMMUNITY-MIB) module, defined in RFC 2576, in Cisco IOS software.

The SNMPv1/v2c Message Processing Model and Security Model require mappings between parameters used in SNMPv1 and SNMPv2c messages and the version independent parameters used in the Simple Network Management Protocol (SNMP) architecture. The SNMP Community MIB contains objects for mapping between these community strings and version-independent SNMP message parameters.

The mapped parameters consist of the SNMPv1/v2c community name and the SNMP securityName and contextEngineID/contextName pair. This MIB provides mappings in both directions, that is, a community name may be mapped to a securityName, contextEngineID, and contextName, or the combination of securityName, contextEngineID, and contextName may be mapped to a community name. This MIB also augments the snmpTargetAddrTable with a transport address mask value and a maximum message size value.

For implementation details, refer to the SNMP-COMMUNITY-MIB.my file, available through Cisco.com at ftp://ftp.cisco.com/pub/mibs/v2/.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release ports the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Speech Recognition and Synthesis for Voice Applications

The Speech Recognition and Synthesis for Voice Applications feature adds support for automatic speech recognition (ASR) and text-to-speech (TTS) capabilities for VoiceXML and TCL applications. This feature provides interfaces to ASR and TTS media servers using Media Resource Control Protocol (MRCP), an application-level protocol developed by Cisco and its ASR and TTS media server partners. Client devices that process audio or video streams use MRCP to control media resources on the external ASR and TTS servers.

Refer to the following documents for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ivrapp/index.htm.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/rel_docs/vxmlprg/index.htm.

Static Cache Entry for IPv6 Neighbor Discovery

The Static Cache Entry for IPv6 Neighbor Discovery feature enables the configuring of static entries in the IPv6 neighbor discovery cache, which provides functionality in IPv6 that is equivalent to static Address Resolution Protocol (ARP) entries in IPv4. Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process. Cisco IOS software uses static ARP entries in IPv4 to translate 32-bit IP addresses into 48-bit hardware addresses. In IPv6, Cisco IOS software uses static entries in the IPv6 neighbor discovery cache to translate 128-bit IPv6 addresses into 48-bit hardware addresses.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/ftipv6s.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

Survivable Remote Site Telephony Version 2.0

The Survivable Remote Site Telephony Version 2.0 feature was previously released in Cisco IOS Release 12.2(8)T. In Cisco IOS Release 12.2(11)T, there are minor enhancements to this feature, which is now referred to as Survivable Remote Site Telephony Version 2.01. Refer to the following document for information about the enhancements added to this release:

http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/srs/fallbak2.htm.

T.37/T.38 Fax Gateway

This feature adds Store-and-Forward Fax to the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850. Store-and-Forward Fax, previously documented in the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2, enables routers to send and receive faxes across packet-based networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/index.htm.

Note

The T.37/T.38 Fax Gateway feature was originally supported in Cisco IOS Release 12.1(5)T on the Cisco AS5300 platform. In Cisco IOS Release 12.2(8)T, support was added on the Cisco 1751 router under the feature title T.37 Store-and-Forward Fax for Cisco 1751 Modular Access Routers and for the Cisco 2600 series and Cisco 3600 series routers under the feature title T.37 Store-and-Forward Fax for the Cisco 2600 Series and Cisco 3600 Series Routers. In this release, support for the T.37/T.38 Fax Gateway feature has been added to the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

T.38 Fax Relay for VoIP H.323

The T.38 Fax Relay for VoIP H.323 feature provides standards-based Fax Relay protocol support on Cisco 2600 series, Cisco 3600 series, Cisco 7200 series and Cisco MC3810 series multiservice gateways. The Cisco proprietary Fax Relay solution is sometimes not an ideal solution for Enterprise and Service Provider customers who have implemented a mixed vendor network. Because the T.38 Fax Relay protocol is standards based, Cisco gateways and gatekeepers will now be able to interoperate with third-party T.38-enabled gateways and gatekeepers in a mixed vendor network where real time Fax Rel capabilities are required.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/faxapp/index.htm.

Note

This feature was originally introduced in Cisco IOS Release 12.1(3)T. This release ports the feature into the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

TCL IVR 2.0 Call Initiation and Callback

The TCL IVR 2.0 Call Initiation and Callback feature allows Tool Command Language (TCL) Interactive Voice Response (IVR) applications to make outbound calls without specifying an incoming call leg in the setup command.

The TCL IVR 2.0 Call Initiation and Callback feature modifies the following TCL IVR Version 2.0 verbs:

- The **leg setup** command.
- The **aaa authorize** command.

In addition, the following new information tags were added to support the above changes:

- infotag get leg_guid
- infotag get leg_incoming_guid
- infotag get aaa_new_guid

Finally, the following additions were made to the callInfo array:

- CallInfo(guid)
- CallInfo(incomingGuid)

Refer to the following *TCL IVR API Command Reference* for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2/chapter3.htm.

TCL IVR Disconnect Cause-Code Manipulation

The leg disconnect command disconnects one or more call legs that are not part of any connection. The cause_code argument, which has been added in Cisco IOS Release 12.2(1)T, is an integer ISDN cause code for the disconnect. It is of the form di-xxx or just xxx, where xxx is the ISDN cause code. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(1)T..This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

TCL-Enabled Signaling Parameter Mapping

The TCL-Enabled Signaling Parameter Mapping feature provides control over call signaling information elements from a Tool Command Language (TCL) Interactive Voice Response (IVR) script to make the Cisco Media-Gateway (that is, the Cisco AS5300 and Cisco AS5800 platforms) interoperable with British Telecom and France Telecom networks. New parameters were introduced under the **set callinfo** command. Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2/chapter3.htm.

TCP Window Scaling

TCP Window Scaling adds support for the Window Scaling extension option in RFC 1323. To improve TCP performance in network paths with a large bandwidth-delay product, Long Fat Networks (LFNs), a larger window size is recommended. This TCP Window Scaling enhancement provides that support.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/tcpwslfn.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Timer and Retry Enhancements for L2TP and L2F

The Timer and Retry Enhancements for L2TP and L2F feature allows the user to configure certain adjustable timers for the L2TP and L2F protocols. For L2F, the settings for control packet retries and control packet timeouts are now both configurable. Initial tunnel packet retries and initial tunnel packet timeouts are now configurable for both the L2F and L2TP protocols.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftretreh.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T as L2TP and L2F Timer and Retry Enhancement. This release is porting the feature into the Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.

Trustpoint CLI

The Trustpoint CLI feature introduces the **crypto ca trustpoint** command, which combines and replaces the functionality of the existing **crypto ca identity** and **crypto ca trusted-root** commands.

Although both of the existing commands allow you to declare the certification authority (CA) that your router should use, only the **crypto ca identity** command supports enrollment (the requesting of a router certificate from a CA). With the **crypto ca trustpoint** command, you can declare the CA and specify any characteristics for the CA that the existing commands supported.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fttrust.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5800 platforms.

Tunnel Type of Service (ToS)

The Tunnel Type of Service (ToS) feature allows you to configure the ToS and Time-to-Live (TTL) byte values in the encapsulating IP header of tunnel packets for an IP tunnel interface on a router. The Tunnel ToS feature is supported on Cisco Express Forwarding (CEF), fast switching, and process switching forwarding modes.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s17/12s_tos.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release ports the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

Universal Port Resource Pooling for Voice and Data Services

With Cisco Resource Pool Manager (RPM), telephone companies and Internet service providers (ISPs) can share dial resources for wholesale and retail dial network services in a single network access server (NAS) or across multiple NAS stacks. Call management and call discrimination can be configured to occur before the call is answered, and customers are differentiated by using configurable customer profiles that are based on the dial number identification service (DNIS) and call type determined at tl time of an incoming call. As a result, Cisco RPM enables service providers to count, control, and manage resources and provide accounting for shared resources when implementing different service-level agreements.

The Universal Port Resource Pooling for Voice and Data Services feature enables service providers to mix voice and data services using resource pool management. With the implementation of the new **voice** command in resource-pool profile service configuration mode, a resource group with voice service is designated under a particular customer profile, and voice resource pool service is enabled after resource pool management is configured.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xa/122xa_2/ftuprp.htm.

V.44 LZJH Compression for Cisco AS5300 and Cisco AS5800 Universal Access Servers

Note This feature is for use with Cisco MICA portware.

The V.44 LZJH Compression for Cisco AS5300 and Cisco AS5800 Universal Access Servers feature introduces the V.44 Lempel-Ziv-Jeff-Heath (LZJH) compression algorithm International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard on Cisco MICA portware platforms.

V.44 LZJH is a new compression standard based on Lempel-Ziv that uses a new string-matching algorithm that increases upload and download speeds to make Internet access and web browsing faster. The V.44 call success rate (CSR) is similar to V.42bis with significant compression improvement for most file types, including HTML files. V.44 applies more millions of instructions per second (MIPS) than V.42bis toward the same application data stream and yields better compression rates in almost any data stream in which V.42bis shows positive results.

V.44 supports automatic switching between compressed and transparent modes on Cisco MICA portware platforms. Automatic switching allows overall performance gains without loss in throughput for file streams that are not compressible.

V.44 is globally controlled through dialed number identification service (DNIS), calling line ID (CLID), and resource pool manager server (RPMS) virtual groups, and performance improvement is determined by the LZJH algorithms. The Cisco MICA portware is responsible for the ITU implementation of V.44 and the collection of statistics related to the new feature.

To support V.44 LZJH compression, the control switch module (CSM) has been modified. MIBs that show the status of V.42bis have been extended to show V.44 configuration status. New disconnect reasons help manage V.44 session status and debugging.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/122xb2_2/ftv44mca.htm.

V.44 LZJH Compression for Cisco AS5350, Cisco AS5400, and Cisco AS5850 Universal Gateways and Cisco AS5800 Universal Access Servers

Note This feature is for use with Cisco NextPort firmware.

The V.44 LZJH Compression for Cisco AS5350, Cisco AS5400, and Cisco.AS5850 Universal Gateways and Cisco AS5800 Universal Access Servers feature introduces the V.44 Lempel-Ziv-Jeff-Heath (LZJH) compression algorithm International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard on Cisco MICA portware platforms.

V.44 LZJH is a new compression standard based on Lempel-Ziv that uses a new string-matching algorithm that increases upload and download speeds to make Internet access and web browsing faster. The V.44 call success rate (CSR) is similar to V.42bis with significant compression improvement for most file types, including HTML files. V.44 applies more millions of instructions per second (MIPS) than V.42bis toward the same application data stream and yields better compression rates in almost any data stream in which V.42bis shows positive results.

V.44 supports automatic switching between compressed and transparent modes on Cisco MICA portware platforms. Automatic switching allows overall performance gains without loss in throughput for file streams that are not compressible.

V.44 is globally controlled through dialed number identification service (DNIS), calling line ID (CLID), and resource pool manager server (RPMS) virtual groups, and performance improvement is determined by the LZJH algorithms. The Cisco MICA portware is responsible for the ITU implementation of V.44 and the collection of statistics related to the new feature.

To support V.44 LZJH compression, the control switch module (CSM) has been modified. MIBs that show the status of V.42bis have been extended to show V.44 configuration status. New disconnect reasons help manage V.44 session status and debugging.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/122xb2_2/ft_v44.htm.

V.92 Modem on Hold for Cisco AS5300 and Cisco AS5800 Universal Access Servers

Note This feature is for use with Cisco MICA portware.

The V.92 Modem on Hold for Cisco AS5300 and Cisco AS5800 Universal Access Servers introduces the V.92 International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard Modem on Hold (MOH) feature with Cisco MICA portware.

To remain current with industry needs, the ITU-T V.90 modem standard recommendations have been enhanced. The new standard, V.92, meets the need for a digital modem and analog modem pair on the Public Switched Telephone Network (PSTN). V.92 improves the upstream data signaling rate and adds new features that enhance modem usability.

V.92 is implemented at the modem level as new modem protocols and standards. The new V.92 features co-reside with existing portware features and have no impact on the hardware configuration of either the HMM or DMM (including memory requirements). Cisco IOS software is responsible for controlling the features and displaying the new statistics. V.92 and V.44 support is bound with the rest of the Cisco IOS device driver components.

V.92 Modem on Hold allows a dial-in customer to suspend a modem session to answer an incoming voice call or to place an outgoing call while engaged in a modem session. When the dial-in customer uses Modem on Hold to suspend an active modem session to engage in an incoming voice call, the Internet service provider (ISP) modem listens to the original modem connection and waits for the dial-in customer's modem to resume the connection. When the voice call ends, the modem signals the telephone system to end the second call and return to the original modem connection, then the modem signals the ISP modem that it is ready to resume the modem call. Both modems renegotiate the connection, and the original exchange of data continues.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/122xb2_2/ft92mmoh.htm.

V.92 Modem on Hold for Cisco AS5350, Cisco AS5400, and Cisco AS5850 Universal Gateways and Cisco AS5800 Universal Access Servers

Note This feature is for use with Cisco NextPort firmware.

The V.92 Modem on Hold for Cisco AS5350, Cisco AS5400, and Cisco AS5850 Universal Gateways and Cisco AS5800 Universal Access Servers feature introduces the V.92 International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard Modem on Hold (MOH) feature with Cisco MICA portware.

To remain current with industry needs, the ITU-T V.90 modem standard recommendations have been enhanced. The new standard, V.92, meets the need for a digital modem and analog modem pair on the Public Switched Telephone Network (PSTN). V.92 improves the upstream data signaling rate and adds new features that enhance modem usability.

V.92 is implemented at the modem level as new modem protocols and standards. The new V.92 features co-reside with existing portware features and have no impact on the hardware configuration of either the HMM or DMM (including memory requirements). Cisco IOS software is responsible for controlling the features and displaying the new statistics. V.92 and V.44 support is bound with the rest of the Cisco IOS device driver components.

V.92 Modem on Hold allows a dial-in customer to suspend a modem session to answer an incoming voice call or to place an outgoing call while engaged in a modem session. When the dial-in customer uses Modem on Hold to suspend an active modem session to engage in an incoming voice call, the Internet service provider (ISP) modem listens to the original modem connection and waits for the dial-in customer's modem to resume the connection. When the voice call ends, the modem signals the telephone system to end the second call and return to the original modem connection, then the modem signals the ISP modem that it is ready to resume the modem call. Both modems renegotiate the connection, and the original exchange of data continues.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/122xb2_2/ftv92moh.htm.

V.92 Quick Connect for Cisco AS5300 and Cisco AS5800 Universal Access Servers

Note This feature is for use with Cisco MICA portware.

The V.92 Quick Connect for Cisco AS5300 and Cisco AS5800 Universal Access Servers feature introduces the V.92 International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard Quick Connect (QC) feature with Cisco MICA portware platforms.

V.92 Quick Connect speeds up the client-to-server startup negotiation, reducing the overall connect time up to 30 percent. The client modem retains line condition information and characteristics of the connection of the Internet service provider (ISP), which reduces connect time by avoiding some of the initial signal handshaking.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/122xb2_2/ft92mqc.htm.

V.92 Quick Connect for Cisco AS5350, Cisco AS5400, and Cisco AS5850 Universal Gateways and Cisco AS5800 Universal Access Servers

Note This feature is for use with Cisco NextPort firmware.

The V.92 Quick Connect for Cisco AS5350, Cisco AS5400, and Cisco AS5850 Universal Gateways and Cisco AS5800 Universal Access Servers feature introduces the V.92 International Telecommunication Union Telecommunication Standardization Sector (ITU-T) standard Quick Connect (QC) feature with Cisco MICA portware platforms.

V.92 Quick Connect speeds up the client-to-server startup negotiation, reducing the overall connect time up to 30 percent. The client modem retains line condition information and characteristics of the connection to the Internet service provider (ISP), which reduces connect time by avoiding some of the initial signal handshaking.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/122xb2_2/ftv92qc.htm.

VoAAL2 Profile 9 Support for Broadband Loop Emulation Services Specification Interoperability

The VoAAL2 Profile 9 Support for Broadband Loop Emulation Services Specification Interoperability feature allows the Cisco IAD2420 series integrated access device (IAD) to provide Voice over ATM Adaptation Layer 2 (VoAAL2) Profile 9 using G.711 u-law or G.711 a-law with a 44-byte voice payload. Profile 9 is part of the Broadband Loop Emulation Services (BLES) specification put forth by the ATM Forum. This feature enables Cisco IAD2420 series IADs to offer standards-based interoperability with V5.2 and GR.303 VoAAL2 gateways from various third party vendors that are BLES compliant. The Profile 9 feature allows the Cisco IAD2420 series IADs to deliver business-class voice services from Class 5 switches over T1 ATM and xDSL WAN links. Profile 9 establishes the foundation for accepting packet voice architectures for the carriers and allows the transition to the call agent architectures.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_iadp9.htm
.

Voice Application Access To SS7 Signaling

The Voice Application Access To SS7 Signaling feature provides a means of transporting ISUP signaling messages from SS7 networks to VoIP networks. ISUP messages and parameters are converted to Generic Transparency Descriptor (GTD) format and transported by the underlying call signalling messages to each node transited by the call.

Refer to the following document for information about the information tags that are associated with this feature:

http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/access/acs_serv/vapp_dev/tclivrv2/chapter4.htm.

Voice DSP Control Message Logger

The Voice DSP Control Message Logger feature provides improved debugging capabilities through Cisco IOS software by allowing you to log control messages that pass through the Cisco IOS software and TI-based voice DSP firmware on the Host Port Interface (HPI). The logged messages can later be examined when voice problems are diagnosed.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftvdsplg.htm.

Voice over IP Q.SIG Network Transparency

Integration of Q.SIG with the Cisco AS5400 universal access server enables Cisco voice switching services to connect private branch exchanges (PBXs), key systems (KTs), and central office switches (COs) that communicate by using the Q.SIG protocol.

The Q.SIG protocol is a variant of ISDN D-channel voice signaling. It is based on the ISDN Q.921 and Q.931 standards and is becoming a worldwide standard for PBX interconnection. By using Q.SIG signaling, the Cisco AS5300 can route incoming voice calls from a private integrated services network exchange (PINX) across a wide-area network (WAN) to a peer Cisco AS5400, which can then transport the signaling and voice packets to a second PINX.

Q.SIG on the AS5400 allows the user to place Q.SIG calls into and receive Q.SIG calls from Cisco Voice-over-IP (VoIP) networks. The Cisco packet network appears to PBXs as a large, distributed transit PBX that can establish calls to any destination served by a Cisco voice node. The switched voice connections are established and torn down in response to Q.SIG control messages that come over an ISDN PRI D channel. The Q.SIG message is passed transparently across the IP network and the message appears to the attached PINXs as a transit network. The PINXs are responsible for processing and provisioning the attached services.

Note This feature was originally introduced in Cisco IOS Release 12.0(7)T on the Cisco AS5300 platform. This release ports the feature into the Cisco AS5400 platform.

VoiceXML For Cisco IOS

Applications written in Voice eXtensible Markup Language (VoiceXML) provide access through a voice browser to content and services over the telephone, just as Hypertext Markup Language (HTML) provides access through a web browser running on a PC. The universal accessibility of the telephone and its ease of use makes VoiceXML applications a powerful alternative to HTML for accessing the information and services of the World Wide Web.

The Cisco IOS VoiceXML feature provides a platform for interpreting VoiceXML documents. When a telephone call is made to the Cisco VoiceXML-enabled gateway, VoiceXML documents are downloaded from web servers, providing content and services to the caller, typically in the form of pre-recorded audio in an IVR application. Customers can access online business applications over the telephone, providing for example, stock quotes, sports scores, or bank balances.

VoiceXML brings the advantages of web-based development and content delivery to voice applications. It is similar to HTML in its simplicity and in its presentation of information. The Cisco IOS VoiceXML feature is based on the *W3C VoiceXML 2.0 Working Draft* and is designed to provide web developers great flexibility and ease in implementing VoiceXML applications.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ivrapp/index.htm.

VoiceXML SS7 ISUP Session Variables

The ISUP signaling message set used in SS7 networks contains information that is used for call establishment, routing, and billing functions. To help transport these messages from SS7 networks (using ISUP based messages) to VoIP networks (using H.323 and SIP based messages), ISUP messages and parameters are represented in generic transparency descriptor (GTD) format and transported by the underlying call signaling messages to each node transited by the call. These GTD parameters and fields are extracted and mapped to TCL and VoiceXML variables for access by Tool Command Language (TCL) and VoiceXML scripts.

VoiceXML Media Volume and Rate Controls

With the VoiceXML Media Volume and Rate Controls feature, the volume of audio prompts played out by VoiceXML applications can now be adjusted during playback. Audio prompts that are played out from memory or chunked transfer mode using G.711 or GSM-FR codecs can also be speeded up or slowed down. A VoiceXML variable contains the rate and duration of the last prompt that was played. The rate and volume of prompts is controlled by using Cisco-specific attributes in the VoiceXML document.

VoiceXML Transfer Enhancements

THe VoiceXML Transfer Enhancements feature enhances the transfer functionality in the Cisco VoiceXML implementation by introducing specific Cisco parameters as attributes for the transfer element.

VoiceXML Voice Store and Forward

The VoiceXML Voice Store and Forward feature expands Cisco IOS VoiceXML to include streaming-based recording and playout. It enables the input and processing of form field entries using recorded audio clips, rather than numeric input only. Audio clips can be captured and then submitted to an external web server using HTTP or Real Time Streaming Protocol (RTSP), or to a messaging server using Simple Mail Transfer Protocol (SMTP) for additional processing.

VoIP Call Admission Control using RSVP

The VoIP Call Admission Control Using RSVP feature synchronizes Resource Reservation Protocol (RSVP) procedures with H.323 Version 2 (Fast Connect) setup procedures to guarantee that the required Quality of Service (QoS) for VoIP calls is maintained across the IP network. In older Cisco IOS releases, VoIP gateways used H.323 Version 1 (Slow Connect) procedures when initiating calls requiring bandwidth reservation. This feature, which is enabled by default, allows gateways to use H.323 Version 2 (Fast Connect) for all calls, including those requiring RSVP.

Note This feature was originally introduced in Cisco IOS Release 12.1(5)T. This release ports the feature into the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.

VoIP Interoperability with Cisco Express Forwarding and Policy Based Routing

The VoIP Interoperability with Cisco Express Forwarding and Policy Based Routing feature consists of the following two features:

- VoIP and Cisco Express Forwarding (CEF) Interoperability
- VoIP and Policy Based Routing (PBR) Interoperability

The VoIP Interoperability with Cisco Express Forwarding and Policy Based Routing feature enables CEF for switching voice signaling and voice payloads from voice interfaces to other LAN/WAN interfaces for applications, such as Tollbypass. This feature also enables Policy Based Routing of VoIP traffic that originates or terminates on the specified voice gateways and introduces voice packet Differentiated Services Code Point (DSCP) marking for Media Gateway Control Protocol (MGCP) voice gateways.

This feature modifies the Voice over IP (VoIP) and interactive voice response (IVR) programming so that they can interoperate with features that are supported only in the CEF path (not in the fast switching path that VoX uses). Voice and IVR currently only work in the fast path on the routers where they are originated and terminated (Voice and IVR on "transit" routers are just data packets and of course can be CEF switched). Cisco Express Forwarding

Cisco Express Forwarding (CEF) is advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.

Although you can use CEF in any part of a network, it is designed for high-performance, highly resilient Layer 3 IP backbone switching.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ft_cef26.htm .

VoIP Gatekeeper Trunk and Carrier Based Routing Enhancements

The VoIP Gatekeeper Trunk and Carrier Based Routing Enhancements feature implements the capability to report the Public Switched Telephone Network (PSTN)-side interfaces for incoming and outgoing calls to the H.323 gatekeeper and to the peer H.323 gateway and endpoint. The feature permits identification, by means of labeling individual PSTN trunks or trunk groups, the circuit that is sending a call. The software routes the call to a specific outbound circuit using some criteria, such as inbound circuit, time period, or cost, and then forwards the call to a circuit that is connected to the specified outbound carrier.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftgkrenb.htm .

VoIP Gateway Trunk and Carrier Based Routing Enhancements

Voice wholesalers use multiple ingress and egress carriers to route traffic. A call that comes in to a gateway on a particular ingress carrier must be routed to an appropriate egress carrier. As networks grow and become more complicated, the dial plans needed to route the carrier traffic efficiently become more complex and the need for carrier sensitive routing (CSR) increases.

The VoIP Gateway Trunk and Carrier Based Routing Enhancements feature implements Carrier Sensitive Routing (CSR) for Cisco voice gateways. The VoIP Gateway Trunk and Carrier Based Routing Enhancements feature adds the following routing features:

- Implementation of trunk groups and enhanced key matches on several platforms and interfaces
- Reduction of the number of dial peers in a dial plan by using profile aggregation and multiple trunk group supports
- Enhanced hunting schemes
- Carrier ID support
- Trunk group label support
- Number translation profiles per trunk group, source IP group, voice port, and dial peer
- Dial peer support of multiple trunk groups with translations per trunk group
- ENUM support
- Source IP groups
- Voice over IP (VoIP) access list control
- Enhanced translation rules in SED (stream editor) regular expressions
- Incoming call blocking
- Cisco IVR 2.0 support for carrier ID based dial peer matching, incoming call blocking, and dial peer number translation
- Call detail record (CDR) support
- Virtual Private Network (VPN) source routing (also referred to as static or basic carrier routing).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftgwrepg.htm

VoIP Outgoing Trunk Group Identification and Carrier ID for Gateways

The VoIP Outgoing Trunk Group Identification and Carrier ID for Gateways feature provides an enhancement to Registration, Admission, and Status (RAS) Admission Confirmation and Location Confirm messages. RAS messages include a circuitInfo field that provides trunk group label or carrier ID information for remote endpoints (gateways) in H.323 networks. The Voice over IP (VoIP) Outgoing Trunk Group Identification and Carrier ID for Gateways feature also adds trunk group label and carrier ID support for the alternate endpoint field in the Gatekeeper Transaction Message Protocol (GKTMP Response Admission Request (ARQ), Admission Confirmation (ACF), Location Request (LRQ), and Location Confirm (LCF) messages.

The **carrier-id** keyword and *carrier-name* arguments were introduced for the **endpoint alt-ep h323id** command in Cisco IOS Release 12.2(11)T.

VPDN Group Session Limiting

Before the introduction of the VPDN Group Session Limiting feature, you could only globally limit the number of virtual private dialup network (VPDN) sessions on a router with limits applied equally to all VPDN groups. Using the VPDN Group Session Limiting feature, you can limit the number of VPDN sessions allowed per VPDN group. This feature is implemented with the introduction of the

session-limit *number* command in VPDN group configuration mode. VPDN group session limiting is applied after the global VPDN session limiting (which is configured via the **vpdn session-limit** *session* command in configuration mode) is enforced.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t11/ftvpdngs.htm

Note This feature was originally introduced in Cisco IOS Release 12.2(4)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP

The VPN Routing Forwarding (VRF) Framed Route (Pool) Assignment via PPP feature introduces support to make the following RADIUS attributes VRF aware: attribute 22 (Framed-Route), a combination of attribute 8 (Framed-IP-Address) and attribute 9 (Framed-IP-Netmask), and the Cisco VSA route command. Thus, static IP routes can be applied to a particular VRF routing table rather than the global routing table.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

WRED Enhancement—Explicit Congestion Notification (ECN)

Currently, the congestion control and avoidance algorithms for TCP are based on the idea that packet loss is an appropriate indication of congestion on networks that transmit data using the best-effort service model. When a network uses the best-effort service model, the network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. However, these algorithms and the best-effort service model are not suited to applications that are sensitive to delay or packet loss (for instance, interactive traffic including Telnet, web browsing, and transfer of audio and video data). Weighted random early detection (WRED), and by extension, Explicit Congestion Notification (ECN), helps to solve this problem.

To indicate congestion, WRED drops packets on the basis of the average queue length exceeding a specific threshold value. ECN is an extension to WRED in that ECN marks packets instead of dropping them when the average queue length exceeds a specific threshold value. When configured with the WRED Enhancement—Support for Explicit Congestion Notification feature, routers and end hosts would use this marking as a signal that the network is congested and slow down sending packets.

This feature provides an improved method for congestion avoidance by allowing the network to mark packets for transmission later, rather than dropping them from the queue. Marking the packets for transmission later accommodates applications that are sensitive to delay or packet loss and provides improved throughput and application performance.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftwrdecn.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

X.25 Over TCP Profiles

The Cisco X.25 over TCP (XOT) service was originally developed as an X.25 class of service that was only designed to switch X.25 traffic across an IP network. This service allowed network administrators to connect X.25 devices across the rich connectivity and media features available to IP traffic. XOT uses a set of default parameters to make this type of network easy to design.

When the XOT' capabilities were enhanced to support packet assembler/disassembler (PAD) traffic on an XOT session, network designers saw a need to be able to configure parameters for increased flexibility. For instance, because XOT does not have any physical interfaces that an administrator can configure, PAD over XOT sessions cannot be configured with interface map or facility commands to establish a PAD connection using nondefault values.

The introduction of X.25 profiles for XOT allows the network designer added flexibility to control the X.25 class services of XOT for PAD and XOT switching usage.

Another important aspect of this feature is that it allows you to associate access lists with XOT connections, enabling you to apply security on the basis of IP addresses and to have a unique X.25 configuration for specified IP addresses.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_xotp.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms.

X.25 Record Boundary Preservation for Data Communications Networks

The X.25 Record Boundary Preservation for Data Communications Networks feature enables hosts using TCP/IP-based protocols to exchange data with devices that use the X.25 protocol, retaining the logical record boundaries indicated by use of the X.25 “more data” bit (M-bit).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdcnrbp.htm.

Note This feature was originally introduced in Cisco IOS Release 12.2(8)T. This release is porting the feature into the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.

Hardware Platforms and Modules Newly Supported in Cisco IOS Release 12.2(8)T1

The following hardware platforms and modules are now supported in Cisco IOS Release 12.2(8)T1. These platforms and modules were first introduced in earlier Cisco IOS software releases.

36-Port Ethernet Switch Module for Cisco 2600 Series and Cisco 3600 Series

The 36-Port Ethernet switch network module is a modular, high-density voice network module that provides Layer 2 switching across Ethernet ports. The 36-port Ethernet switch network module has thirty-six 10/100BASE-TX ports, and an optional power module can also be added to provide inline power for Cisco IP telephones.

The 36-port Ethernet switch network module supports the same features as the 16-port Ethernet switch network module introduced in Cisco IOS Release 12.2(8)T.

Cisco 1721 Router

The Cisco 1721 data-only modular access router is an enhanced Cisco = 1720 router that provides higher performance, additional functionality, and increased memory capacity. The router supports WAN access, Virtual Private Network (VPN), and firewall technology for secure Internet, intranet, and extranet access. Cisco 1721 routers also support standards-based Institute of IEEE 802.1Q VLAN routing, which enables enterprises to set up and route between multiple VLANs for additional security in an internal corporate network.

Cisco 2600XM Series Routers

The Cisco 2600XM series provides new product enhancements to the current Cisco 2600 series. The Cisco 2600XM series is available in three performance levels and six base configurations:

- Cisco 2650XM and Cisco 2651MX—up to 40K packets per second (pps), one and two autosensing 10/100 Mbps Ethernet ports
- Cisco 2620XM and Cisco 2621XM—up to 30K pps, one and two autosensing 10/100 Mbps Ethernet ports
- Cisco 2610XM and Cisco 2611XM—up to 20K pps, one and two autosensing 10/100 Mbps Ethernet ports

Each model also has two WAN interface card (WIC) slots, one Network Module slot, and an Advanced Integration Module.

Cisco 2691 Series Router

Cisco IOS Release 12.2(8)T1 supports a new platform, the Cisco 2691 series router.

The Cisco 2691 router is part of the next generation Modular Multiservice platform for deployment of advanced IP Telephony Solutions and Integrated Services. This platform is the fourth in a series of Cisco 2600 products that offer additional performance levels.

The Cisco 2691 provides two 10/100BASE-T Fast Ethernet (FE) ports with one Network Module (NM) slot, three WAN Interface Cards (WICs) slots, and two Advanced Interface Module (AIM) slots. Many of the current NMs, WICs and AIMs used today on the Cisco 2600 and Cisco 3600 series routers are supported on the Cisco 2691 series router.

New Software Features in Cisco IOS Release 12.2(8)T1

The following new features are supported in Cisco IOS Release 12.2(8)T1. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

MPLS Label Switch Controller and Enhancements

The Multiprotocol Label Switching (MPLS) Label Switch Controller (LSC), combined with a slave ATM switch, supports scalable integration of IP services over an ATM network. The MPLS LSC enables the slave ATM switch to:

- Participate in an MPLS network
- Directly peer with IP routers
- Support the IP features in Cisco Internetwork Operating System (IOS) software

This feature was originally introduced in Cisco IOS Release 11.1CT as the Tag Switch Controller. Cisco IOS Release 12.2(8)T1 adds support for the Cisco 8400 IGX Switch with a Universal Router Module as an MPLS ATM-LSR. In addition, support is added for the Virtual Circuit (VC) Merge and MPLS Diff-Serv-aware features.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftlsc.htm.

Virtual Circuit (VC) Merge

The Virtual Circuit (VC) Merge feature allows multiple incoming VCs to be merged into a single outgoing VC. The feature is only available on frame-based connections carrying ATM Adaptation Layer 5 (AAL5) frames consisting of multiple cells. VC Merge helps scale Multiprotocol Label Switching (MPLS) networks, because it allocates only one VC to each destination on a link.

VC merge maps several incoming labels to one single outgoing label. Cells from different virtual channel identifiers (VCIs) traveling to the same destination are transmitted to the same outgoing VC using multipoint-to-point connections.

VC merge allows the switch to transmit cells coming from different VCIs over the same outgoing VCI to the same destination. In other words, VC merge queues AAL5 frames in input buffers until the switch receives the last frame. Then the switch transmits the cells from that AAL5 frame before it sends any cells from other frames. VC merge requires the switch to provide buffering, but no more buffering than is required in IP networks. VC merge slightly delays the transfer of frames; however, VC merge is for IP traffic and not for traffic that requires speed. IP traffic tolerates delays better than other traffic on the ATM network.

Hardware Platforms and Modules Newly Supported in Cisco IOS Release 12.2(8)T

The following hardware platforms and modules are now supported in Cisco IOS Release 12.2(8)T. These platforms and modules were first introduced in earlier Cisco IOS software releases.

1- and 2-Port V.90 Modem WICs for Cisco 2600 and 3600 Series

Three applications are available for the V.90 modem WAN interface card (WIC) on the Cisco 2600 and Cisco 3600 series multiservice platforms.

Remote Router Management and Out-of-Band Access

In this mode, the modem WIC is used as a dial-in modem for remote terminal access to the router's command-line interface (CLI) for configuration, troubleshooting, and monitoring. The modem WIC acts similar to a modem that is connected to the auxiliary (AUX) port of a router, but the integrated nature of the modem WIC greatly decreases customer configuration time and deployment and sustaining costs. Typically, the 1-port modem WIC is used for this application. Connection speeds of up to 33.6 kbps are possible.

Asynchronous Dial-on-Demand Routing and Dial Backup

In this mode, the V.90 modem WIC transports network traffic. When ISDN service is not available and the traffic load does not justify a leased line or Frame Relay connection, asynchronous dial-on-demand routing (DDR) is often the only choice for making a WAN connection. Even at sites that do have a leased line or Frame Relay connection, asynchronous DDR can increase bandwidth during sustained traffic load. In addition, when the primary leased line or Frame Relay link is down during an outage, asynchronous dial backup provides a secondary way to make the WAN connection. Both the 1-port and 2-port versions of the V.90 modem WIC can be used for this application.

Two ports on one modem WIC (or even three or more ports spanning multiple modem WIC cards) can be combined using Multilink PPP (MLP) to increase connection speeds in a scalar manner. Each connection is capable of V.90 speeds (up to 56 kbps) when connecting to a digital V.90 server modem.

Low-Density Analog RAS Access

In this application, the V.90 modem WIC enables the platform to provide the services of a typical small remote access server (RAS). One service allows remote users to dial in and gain access to resources on the LAN (or even across the WAN). The analog modems in the modem WIC allow dial-in connection speeds of up to 33.6 kbps, but MLP can bind multiple links together and increase the throughput.

Another service allows PCs (running Cisco DialOut Utility) on the LAN to use the modems for dial-out. Users can connect to other modems (bulletin boards, AOL, ISPs, and so on) or fax machines. The modem WIC allows dial-out connection speeds of up to 56 kbps when dialing a digital V.90 server modem or up to 33.6 kbps when dialing another analog modem. Fax calls connect at up to 14.4 kbps.

Typical RAS deployments with the V.90 modem WIC use the 2-port modem version. With enough slots, the V.90 modem WIC can be used to scale to up to 24 modems in a Cisco 3660 multiservice platform.

There is no limit for lines in the MLP bundle with WICs and population of WICs on any Cisco 2600 series or Cisco 3600 series multiservices platforms.

Additional Information

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft12pwi8.htm.

8FXO DID for IAD24xx Platform

Note The 8FXO DID for IAD24xx Platform feature is also known under the feature title Direct Inward Dialing for Cisco IAD2420 Series Integrated Access Devices.

Direct Inward Dialing (DID) is a service offered by telephone companies that enables callers to dial directly to an extension on a private branch exchange (PBX) without the assistance of an operator or automated call attendant. This service makes use of DID trunks, which forward only the last three to five digits of a phone number to the PBX. If, for example, a company has a PBX with extensions 555-1000 to 555-1999, and a caller dials 555-1234, the local central office (CO) would forward 234 to the PBX. The PBX would then ring extension 234. This entire process is transparent to the caller.

The Foreign Exchange Office (FXO) ports on the analog FXO voice module supports the Direct Inward Dialing (DID) for Cisco IAD2420 platform. An eight-port FXO voice interface module for the Cisco IAD2420 platform provides higher FXO port density than was previously available in the Cisco IAD2420 platform. These analog voice ports can be used to support analog voice connections from the Cisco IAD2420 chassis to the PBX on the CO side of the interface.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdidiad.htm.

16-Port Ethernet Switch Module for Cisco 2600 Series and Cisco 3600 Series

The16-Port Ethernet switch network module is a modular, high-density voice network module that provides Layer 2 switching across Ethernet ports. The 16-port Ethernet switch network module has sixteen 10/100BASE-TX ports, and an optional power module can also be added to provide inline power for Cisco IP telephones.

Features included on this network module include the following:

- Broadcast/Multicast Suppression
- Classless InterDomain Routing (CIDR) IP Default Gateway
- IEEE 802.1Q ISL VLAN Mapping
- IEEE 802.1Q Tunneling
- IEEE 802.1Q VLAN Trunking
- IEEE 802.3x Flow Control
- MAC Address Filtering
- Spanning Tree Protocol-Backbone Fast Convergence
- Spanning Tree Protocol-Portfast Guard
- Spanning Tree Protocol-Uplink Fast Convergence
- Switch Port Analyzer (SPAN)
- Switch Port Analyzer (SPAN)—Disable Receive Traffic Destination Port
- Switch Port Analyzer (SPAN)—Multiple Source Port Selection
- Jumbo Frames

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xt/122xt_2/ft1636nm.htm.

7100 PA Support

The 7100 PA is a port of support for the following features and port adapters on the Cisco 7100: Turbo ACLs, cRTP Acceleration, PA-GE, PA-MC-2T1, PA-MC-2E1/120, PA-POS, PA-MC-4T1, PA-MC-8T1, PA-MC-8E1, PA 2FE, PA-T3+, and PA-2T3+.

AIM-ATM, AIM-VOICE-30, and AIM-ATM-VOICE-30 on the Cisco 2600 Series and Cisco 3660

Three types of Advanced Integration Modules (AIMs) provide components that provide segmentation and reassembly (SAR) of packets for ATM transport over a WAN and voice digital signal processing (DSP) services. The Cisco 2600 series has one internal slot for an AIM, and the Cisco 3660 has two. The three types of AIMs are as follows:

- AIM-ATM—A High-Performance ATM AIM that enables voice and data traffic to be carried over ATM networks using ATM Adaptation Layer 2 (AAL2) and ATM Adaptation Layer 5 (AAL5) encapsulation when installed in Cisco 2600 series or Cisco 3660 routers. If used in conjunction with a T1/E1 multiflex trunk voice/WAN interface card (VWIC-MFT) for circuit-mode data and frame-mode data over ATM infrastructures, it supports up to four T1 or E1 WAN interfaces. These interfaces may be four independent links or four inverse multiplexing over ATM (IMA) groups. When using the voice DSP capability of a digital T1/E1 packet voice trunk network module (NM-HDV) and a T1/E1 multiflex trunk VWIC, it supports as many as 30 channels of compressed voice over a T1/E1 trunk using AAL2 or AAL5. Analog Voice over ATM (VoATM) is enabled with a voice/fax network module (NM-1V or NM-2V) and a voice interface card, which support as many as four analog voice calls using AAL5. The following voice interface cards are supported: FXS, FXO, Analog-DID, E&M, and BRI.
- AIM-VOICE-30—An advanced integration module capable of supporting up to 30 voice or fax channels when used with one of the T1/E1 voice/WAN interface cards (such as VWIC-1T1). This AIM includes powerful digital signal processors (DSPs) that are used for a number of voice processing tasks such as voice compression and decompression, voice activity detection or silence suppression, and private branch exchange (PBX) or public switched telephone network (PSTN) signaling protocols. By using the AIM-VOICE-30 in a Cisco 2600 series router, customers can support Voice over IP (VoIP) or Voice over Frame Relay (VoFR) while the router's network module slot is left open for other functions such as asynchronous or synchronous serial concentration. When used in combination with one of the various ATM network modules, VoATM or VoIP over ATM can be provisioned using AAL5 and Voice over AAL2 (VoAAL2).
- AIM-ATM-VOICE-30—A combined ATM and DSP AIM that supports voice over ATM (VoATM), voice over IP (VoIP), and voice over Frame Relay (VoFR). It supports as many as four T1 or E1 trunks when installed in a Cisco 2600 series or Cisco 3660 router. This AIM is used in combination with one T1/E1 multiflex trunk interface (VWIC-MFT) to provide PBX or PSTN signaling protocols. It uses VoAAL2 (ITU I.366.1/I.363.2) and VoAAL5 and does not require use of a digital T1/E1 packet voice trunk network module. This AIM has an onboard ATM coprocessor for increased AAL2 and AAL5 performance and for as many as four IMA groups, enabling fractional T3 or E3 bandwidth performance.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_04gin.htm.

Analog Station Interface (ASI) Cards

Analog station interface (ASI) cards enable you to connect to analog telephones, fax machines, and teleconferencing stations. The following two ASI cards are available:

- ASI 81—Contains an 8-port Foreign Exchange Station (FXS) module and any one of the VIC/WIC/VWIC modules that support digital and analog voice trunks and WAN routing interfaces, completely integrating voice and data networking.
- ASI 160—Contains a 16-port FXS module.

ATM OC-12 Port Adapter

Platforms: Cisco 7500/RSP series with Versatile Interface Processor (VIP)

The ATM OC-12 Port Adapter is a dual-width ATM port adapter that provides a single-port, 622.08 Mbps connection from Cisco 7500 series routers to any ATM switch. The PA-A3 OC-12 includes two hardware versions (PA-A3-OC12MM and PA-A3-OC12SMI) that support the following standards-based physical interfaces:

- OC-12c/STM-4 multimode
- OC-12c/STM-4 single-mode intermediate reach

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/6228oc12/6228ovrn.htm.

Cisco 806 Broadband Gateway Router

The Cisco 806 Broadband Gateway Router adds business-class functionality to affordable broadband access for small offices and corporate telecommuters. Through the power of Cisco IOS technology, the Cisco 806 provides business-class security, remote management, and quality of service capabilities. These value-added features, with the proven reliability of Cisco IOS technology, provide the mission-critical networking required by today's agile businesses.

Cisco 1721 Router

The Cisco 1721 data-only modular access router is an enhanced Cisco 1720 router that provides higher performance, additional functionality, and increased memory capacity. The router supports WAN access, VPN, and firewall technology for secure Internet, intranet, and extranet access. Cisco 1721 routers also support standards-based IEEE 802.1Q VLAN routing, which enables enterprises to set up and route between multiple VLANs for additional security in an internal corporate network.

Cisco 3631 Series Router

Cisco IOS Release 12.2(8)T supports a new platform, the Cisco 3631 series router.

The Cisco 3631 is a new midrange router for Data Communication Network (DCN) applications that provides two network modules and two WICs, one Fast Ethernet port, one console port, and an auxiliary port. The Cisco 3631 is two rack units high in an 11-inch NEBS/ETSI-compliant chassis that functions at 70,000 pps.

Cisco 3725 Application Service Router

Cisco IOS Release 12.2(8)T supports a new platform, the Cisco 3725 router.

The Cisco 3725 Series Application Service Router is part of a new family of modular routers that enable flexible and scalable deployment of new e-business applications in an integrated branch office access platform.

The Cisco 3700 series are new access platforms optimized for the modular integration and consolidation of branch applications and services. The Cisco 3725 is a two-rack unit (RU) router equipped with two on-board Fast Ethernet (FE) interfaces, three WAN Interface Card (WIC) slots and two Advanced

Integration Module (AIM) slots, and two network module (NM) slots. The Cisco 3725 also includes optional -48vDC integrated inline power to support IP Telephony when used with an EtherSwitch network module.

Cisco 3745 Application Service Router

Cisco IOS Release 12.2(8)T supports a new platform, the Cisco 3745 router.

The Cisco 3745 Series Application Service Router is part of a new family of modular routers that enable flexible and scalable deployment of new e-business applications in an integrated branch office access platform.

The Cisco 3745 is a three-rack unit (RU) router equipped with two on-board Fast Ethernet (FE) interfaces, three WAN Interface Card (WIC) slots and two Advanced Integration Module (AIM) slots, and two network module (NM) slots. The Cisco 3745 also includes optional 48vDC integrated inline power, internal redundant AC or DC Power options, and Online Insertion and Removal (OIR) capabilities for like network modules.

The Cisco 3700 series is ideal for sites and solutions requiring the highest levels of integration at the edge, such as:

- Integration of flexible routing and low density switching
- Single platform solution for Branch Office IP Telephony and Voice Gateway allowing flexible, incremental migration and service integration
- Consolidation of service infrastructure and high service density in a compact form factor

Cisco High-Density Analog Voice and Fax Network Module

The Cisco High-Density Analog Voice and Fax Network Module provides dual tone multifrequency (DTMF) detection, voice compression and decompression, call progress tone generation, voice activity detection (VAD), echo cancellation, and adaptive jitter buffering for up to 16 ports.

The base card supports four foreign exchange station (FXS) ports. The addition of an eight-port FXS expansion module can increase the capacity to twelve FXS ports. The addition of two four-port FXO expansion modules can increase the capacity to eight FXO ports and four FXS ports. The addition of one each of the FXS and FXO expansion modules can increase the capacity to twelve FXS ports and four FXO ports. The FXO expansion module supports a power failure port, which connects directly to the central office (CO) in case of failure.

The digital signal processors (DSPs) on the network module support up to eight ports of high-complexity codecs or up to sixteen ports of medium-complexity and low-complexity codecs. The number of DSPs must be increased if more than eight ports of high-complexity codecs are needed. In this case, a DSP expansion module must be installed.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xt/122xt_2/ft_hdanm.htm.

Cisco IOS Voice Features on IGX 8400 Series Universal Router Module

The Universal Router Module (URM) is a Cisco IOS-based IP router blade that enables users to provision Voice over IP (VoIP) and Voice over ATM (VoATM) on a Cisco IGX 8400 series platform. The voice and routing capabilities of the URM have been derived from the Cisco 3660, while the ATM capabilities have been derived from the ATM OC/3 network module for the Cisco 2600 series and

Cisco 3600 series routers. The embedded UXM-E processor supports one OC3 ATM port, and the embedded router supports one OC3 ATM port similar to the 1-port OC-3/STM-1 ATM Circuit Emulation Service network module for the Cisco 3600 series routers. These ATM ports are connected to each other internally.

In addition to VoIP and VoATM, IP routing and Cisco IOS command-line interface (CLI) commands, which enable configuration of the voice ports and dial peers, are now available on the Cisco IGX 8400 series platforms.

The URM interoperates with all Cisco IOS-based voice products and supports 30 voice channels with high-complexity codec types and 60 voice channels with medium-complexity codec types. Note that only digital voice ports are supported on the URM; analog ports are not supported.

The URM also provides support for MPLS, IP Security (IPSec), remote embedded router configuration of the URM (a RAS feature), and support for Enterprise Plus features. Using the BC-URI-2FE back card, you can use the URM for data-only access. Also, support for VPN-AIM/HP enables the URM to provide hardware-accelerated encryption for scalable IPSec-VPN networks.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_igxxb.htm.

Digital J1 Voice Interface Card

The J1 interface card provides the proper interface for directly connecting Cisco multiservice access routers to Japanese Private Branch Exchanges (PBXs) that use a J1 interface (2.048 Mbps TDM interface). This interface card supports 30 voice channels per port.

It provides the software and hardware features required to connect to over 80 percent of the Japanese PBXs that use digital interfaces. This new J1 voice interface card (VIC) provides a TTC JJ-20.11 compliant interface between high-density voice network modules (NM-HDV) and a Japanese PBX.

The digital J1 card provides a single-port line interface in a VIC form factor. It is specifically designed to conform to the TTC JJ-20.10-12 standards that define the interface between a PBX and time-division multiplexer (TDM).

For additional information about the Digital J1 Voice Interface Card, refer to the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftj1voip.htm.

G.SHDSL Symmetric DSL Support

Note The G.SHDSL Symmetric DSL Support feature is also known under the feature title 1-Port G.SHDSL WAN Interface Card for Cisco 2600 Series and Cisco 3600 Series Routers.

G.SHDSL is an ATM-based, multirate, high-speed (up to 2.3 MB), symmetrical digital subscriber line technology for data transfer between a single customer premises equipment (CPE) subscriber and a central office.

G.SHDSL is supported on the G.SHDSL WAN interface card (WIC-1SHDSL), a 1-port WAN interface card (WIC) for Cisco 2600 series and Cisco 3600 series routers.

The G.SHDSL WIC is compatible with the Cisco 6015, Cisco 6130, Cisco 6160, and Cisco 6260 Digital Subscriber Line Access Multiplexers (DSLAMs). The DSLAM must be equipped with G.SHDSL line cards that are compatible with the DSL service to be configured.

The G.SHDSL WIC supports ATM Adaptation Layer 2 (AAL2), ATM Adaptation Layer 5 (AAL5), and various classes of service for ATM.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_gdsl8.htm.

Multichannel STM-1 Port Adapter

The Multichannel STM-1 Port Adapter is a high-speed, single-port multichannel STM-1 port adapter. You can configure the PA-MC-STM-1 as a multichannel E1/E0 STM-1 port.

The PA-MC-STM-1 can be configured into 63 individual E1 links. Each E1 link can carry a single channel at full or fractional rates or be broken down into multiple DS0 or nx64 Kbps rates. The PA-MC-STM-1 supports up to three TUG-3/AU-3 transport slots numbered 1 through 3. You can configure each TUG-3/AU-3 to carry 21 SDH TU-12s. Each SDH TU-12 is capable of carrying a channelized E1 frame, which can be unchannelized to nx64-Kbps time slots.

For additional information about the Multichannel STM-1 Port Adapter, refer to the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_stm5.htm.

NM-AIC-64, Contact Closure Network Module

The NM-AIC-64, Contact Closure Network Module (also known as the AIC) is an optional card that expands network management capabilities for customer-defined alarms. The AIC has its own CPU that communicates with the router and external media through serial communication channels. The AIC reduces service provider and enterprise operating costs by providing a flexible, low-cost network solution for migrating existing data communications networks (DCNs) to IP-based DCNs. The AIC provides its users with a single box solution because it can be configured in the same router along with other operations, alarm administration, maintenance management, and provisioning (OAM&P) interfaces.

This feature was first introduced on the Cisco 2600 series and Cisco 3600 series platforms in Cisco IOS Release 12.2(2)XG. For Cisco IOS Release 12.2(8)T, platform support for the Cisco 3631 has been added.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_aicnm.htm.

URM LAN

On the Cisco IGX 8400 series, the Universal Router Module (URM) has been enhanced by new LAN features such as Security and VPN. Installed URMs can be enabled with the new features by upgrading to IGX switch software 9.3.30 and Cisco IOS Release 12.2(2)XX as well as by adding an AIM-VPN daughter module to the URM. Also, a new, price-reduced back card for the URM with 2 FE ports (BC-URI-2FE) for LAN services will be supported. URM together with the voice-enabled back cards (BC-URI-2FE2V-E1/T1) will support the new LAN.

New Software Features in Cisco IOS Release 12.2(8)T

The following new features are supported in Cisco IOS Release 12.2(8)T. Some of these features may have been introduced on other hardware platforms in earlier Cisco IOS software releases.

ACL Authentication of Incoming rsh and rcp Requests

To enable the Cisco IOS software to receive incoming remote shell (rsh) protocol and remote copy (rcp) protocol requests, customers must configure an authentication database to control access to the router. This configuration is accomplished by using the **ip rcmd remote-host** command.

Currently, when using this command, customers must specify the local user, the remote host, and the remote user in the database authentication configuration. For users who can execute commands to the router from multiple hosts, multiple database authentication configuration entries must be used, one for each host.

This feature allows customers to specify an access list for a given user. The access list identifies the hosts to which the user has access. A new argument, *access-list*, has been added that can be used with this command to specify the access list.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftauth.htm.

Asynchronous Serial Traffic Over User Datagram Protocol (UDP)

The Asynchronous Serial Traffic Over User Datagram Protocol (UDP) feature provides the ability to encapsulate asynchronous data into UDP packets, and then unreliably transmit this data without needing to establish a connection with a receiving device.

You load the data you want to transmit through an asynchronous port, and then transmit it, optionally, as a multicast or a broadcast. The receiving device(s) can then receive the data whenever it wants. If the receiver ends reception, the transmission is unaffected.

This process is referred to as UDP Telnet (UDPTN), although it does not---and cannot---use the Telnet protocol. UDPTN is similar to Telnet in that both are used to transmit data, but UDPTN is unique in that it does not require that a connection be established with a receiving device.

ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection

The ATM PVC Bundle Enhancement — MPLS EXP-Based PVC Selection feature is an extension to the IP to ATM Class of Service feature suite. The IP to ATM Class of Service feature suite, using virtual circuit (VC) support and bundle management, maps quality of service (QoS) characteristics between IP and ATM. It provides customers who have multiple VCs (with varying qualities of service to the same destination) the ability to build a QoS differentiated network.

The IP to ATM Class of Service feature suite allowed customers to use IP precedence level as the selection criteria for packet forwarding. This new feature now gives customers the option of using th Multiprotocol Label Switching (MPLS) experimental (EXP) level as an additional selection criteria for packet forwarding.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmpls.htm.

ATM Software Segmentation and Reassembly (SAR)

The ATM Software Segmentation and Reassembly (SAR) feature allows the Cisco 2600 series to carry voice and data traffic over ATM networks using ATM Adaptation Layer 2 (AAL2) and AAL5 and allows the Cisco 3660 router to support AAL2 voice traffic.

For the Cisco 2600 series, this feature works in conjunction with the T1/E1 multiflex voice/WAN interface card (VWIC), which is plugged into a WIC slot to provide one ATM WAN interface at a T1/E1 rate supporting up to 24/30 voice channel.

T1/E1 ATM support is a time-to-market feature that helps service providers take advantage of the inherent quality of service (QoS) features of ATM multiservice applications. FR-ATM (FRF.5 and FRF.8) internetworking is supported on the Cisco 2600 series.

On the Cisco 3660, a T1 IMA network module is used as the Inverse Multiplexing ATM (IMA) interface providing a maximum of one ATM IMA interface that supports up to 48/60 voice channels. Up to eight T1/E1s and multiple IMA groups are permitted, but only the first IMA group supports voice over AAL2 for up to 48/60 voice channels.

NM-IMA already supports AAL5 on both the Cisco 2600 series and Cisco 3600 series (not just the Cisco 3660).

The Cisco 2600 Series T1/E1 ATM portion of this feature provides a shared implementation of the ATM features currently available on the Cisco MC3810 with the Cisco 2600 series.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_t1atm.htm.

ATM SVC Troubleshooting Enhancements

The ATM SVC Troubleshooting Enhancements feature introduces the following two new debug commands: **debug atm native** and **debug atm nmba**. These commands can be used to troubleshoot ATM switched virtual circuits (SVCs). The **debug atm nbma** and **debug atm native** commands are used to debug problems with Resource Reservation Protocol (RSVP) SVC creation and teardown. The **debug atm native** command can also be used to debug problems with SVCs created using static maps.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftsvctrb.htm.

BGP Hide Local-Autonomous System

The BGP Hide Local-Autonomous System feature introduces the **no-prepend** keyword to the **neighbor local-as** command. The use of the **no-prepend** keyword allows a network operator to configure a Border Gateway Protocol (BGP) speaker to not prepend the local autonomous system number to any routes that are received from external peers. This feature can be used to help transparently change the autonomous system number of a BGP network and ensure that routes can be propagated throughout the autonomous system, while the autonomous system number transition is incomplete. Because the local autonomous is not prepended to these routes, external routes will not be rejected by internal peers during the transition from one autonomous system number to another.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftbgphla.htm.

BGP Named Community Lists

The BGP Named Community Lists feature introduces a new type of community list called the named community list. The BGP Named Community Lists feature allows the network operator to assign meaningful names to community lists and increases the number of community lists that can be configured. A named community list can be configured with regular expressions and with numbered community lists. All rules of numbered communities apply to named community lists except that there is no limitation on the number of community attributes that can be configured for a named community list.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftbgpncl.htm.

BIP—BSC to IP Conversion for Automated Teller Machines

The Bisync-to-IP (BIP) Conversion for Automated Teller Machines feature enables customers to attach a binary synchronous (bisync) communication automated teller machine to a serial interface on a Cisco router running bisync-to-IP (BIP) protocol translation and then to route the data over a TCP/IP network directly to an IP-based application host.

Call Admission Control for H.323 VoIP Gateways

Call Admission Control for H.323 VoIP Gateways feature set provides the ability to support resource-based call admission control processes. These resources include system resources such as CPU, memory, and call volume and interface resources such as call volume.

If system resources are not available to admit the call, the following two kinds of actions are provided: system denial (which busyouts all of T1 or E1) or per-call denial (which disconnects, hairpins, or plays a message or tone). If the interface-based resource is not available to admit the call, the call is dropped from the session protocol (such as H.323).

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_cac7x.htm.

CDP and ODR Support for ATM PVCs

This feature introduces support for the Cisco Discovery Protocol (CDP) over ATM point-to-point permanent virtual circuits (PVCs). Prior to this release, CDP discovery messages were not supported over ATM interfaces.

CDP is a Cisco proprietary device discovery protocol. Each Cisco device periodically sends messages to a multicast address. These messages advertise information about that device, such as the system ID (name), capabilities, Cisco IOS software version, and the network address of the connected interface. This information will be picked up by any neighboring Cisco devices on the same medium, which are listening for CDP advertisements. The information learned about neighboring devices is available through the Cisco IOS CLI **show cdp** commands and through SNMP monitoring using the CDP MIB.

This feature also adds support for On-Demand Routing (ODR) over ATM PVCs. ODR uses CDP to propagate IP address information in hub-and-spoke topologies. When ODR is enabled, spoke routers automatically advertise their subnets using CDP.

CDP is disabled by default for ATM PVC interfaces. To enable CDP, use the **cdp run** global configuration mode command and the **cdp enable** interface configuration mode command on both ends of the PVC. To enable ODR, use the **router odr** global configuration mode command on the hub router and turn off any dynamic routing protocols in the spoke routers.

For details on configuring CDP, refer to the following documentation:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf015.htm.

For details on configuring ODR, refer to the following documentation:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfodr.htm.

Cisco Discovery Protocol (CDP)— IPv6 Address Family Support for Neighbor Information

The CDP IPv6 Address Family Support for Neighbor Information feature adds the ability to transfer IPv6 addressing information between two Cisco devices using Cisco Discovery Protocol (CDP). CDP in IPv6 functions the same as and offers the same benefits as CDP in IPv4. IPv6 enhancements to CDP allow CDP to exchange IPv6 and neighbor addressing information. IPv6 CDP provides IPv6 information to network management products and provides troubleshooting tools.

CEF-Switched Multipoint GRE Tunnels

The CEF-Switched Multipoint GRE Tunnels feature enables CEF switching of IP traffic to and from multipoint GRE tunnels. Tunnel traffic can be forwarded to a prefix through a tunnel destination when both the prefix and the tunnel destination are specified by the application.

Certificate Autoenrollment

The Certificate Autoenrollment feature allows you to configure your router to automatically request a certificate from the certification authority (CA) that is using the parameters in the configuration. Thus, operator convention is no longer required at the time the enrollment request is sent to the CA server.

Automatic enrollment will be performed on startup for any trustpoint CA that is configured and does not have a valid certificate. When the certificate—which is issued by a trustpoint CA that has been configured for autoenrollment—expires, a new certificate is requested. Although this feature does not provide seamless certificate renewal, it does provide unattended recovery from expiration.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftautoen.htm.

Certificate Enrollment Enhancements

The Certificate Enrollment Enhancements feature introduces five new subcommands to the **crypto ca trustpoint** command—**ip-address** (ca-trustpoint), **password** (ca-trustpoint), **serial-number**, **subject-name**, and **usage**. These commands provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts. (However, the prompting behavior remains the default if this feature is not enabled.) Thus, users can preload all necessary information into the configuration, allowing each router to obtain its certificate automatically when it is booted.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftenrol2.htm.

CISCO-BULK-FILE-MIB Enhancements

The Cisco Bulk File Creation MIB (CISCO-BULK-FILE-MIB.my) is a MIB module for creating and deleting bulk files of SNMP data for file transfer. The CISCO-BULK-FILE-MIB Enhancements feature enhances the Cisco Bulk File Creation MIB to support selective-row-transfer and notification-on-file-creation. Prior to this enhancement, when the MIB was used to dump large tables (for example, the ccHistoryTable), much of the data transfer consisted of duplicated data. This feature allows the SNMP manager to specify a starting row in the SNMP Get request.

This feature also introduces a notification that can be sent when file creation is complete or when there is an error during file creation. Specifically, this feature modifies the CISCO-BULK-FILE-MIB by introducing four new MIB objects (cbfDefineFileNotifyOnCompletion, cbfDefineObjectTableInstance, cbfDefineObjectNumEntries, cbfDefineObjectLastPolledInst) and a new notification object (cbfDefineFileCompletion). For details, refer to the CISCO-BULK-FILE-MIB.my file, available through Cisco.com MIB FTP site at the following URL:

ftp://ftp.cisco.com/pub/mibs/v2/CISCO-BULK-FILE-MIB.my.

Cisco Gateway Management Agent (CGMA) Phase 2

The Cisco Gateway Management Agent (CGMA) Phase 2 feature provides additional enhancements for the Cisco Gateway Management Agent (CGMA) feature. The CGMA provides an eXtensible Markup Language (XML) interface to support real-time management of a Cisco IOS gateway. Currently, gateways provide statistics using Simple Network Management Protocol (SNMP) and do not support real-time polling. The CGMA feature allows gateways to communicate with third-party management applications using XML over TCP/IP.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftcgma2.htm.

Cisco Hoot and Holler over IP

The Cisco Hoot and Holler over IP feature can now be ported to the Cisco 1750, 1751, and 1760 routers in Cisco IOS Release 12.2(8)T. The feature is already available on the Cisco 2600 and 3600 series routers.

Cisco VoIP technology, which was initially focused on traditional PBX toll-bypass applications, can be used to combine hoot and holler networks with data networks. While some customers may have integrated hoot and data to some level in the late 1980s with time-division multiplexing (TDM), this form of integration does not allow for dynamic sharing of bandwidth that is characteristic of VoIP. This dynamic sharing of bandwidth is even more compelling with hoot and holler than with a toll-bypass application because some hoot circuits may be active for an hour or two for morning reports but dead for the rest of the day. The idle bandwidth can be used by the data applications during these long periods of inactivity.

Beginning with Cisco IOS Release 12.1(2)XH, Cisco hoot and holler over IP can be implemented usir Cisco VoIP technology. This solution leverages Cisco IOS expertise in VoIP, quality of service (QoS), and IP multiplexing and is available on Cisco 1750, 1751, and 1760 routers and on Cisco 2600 and 3600 series multiservice routers.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_hhip.htm.

Cisco IOS Firewall Performance Improvements

The Cisco IOS Firewall Performance Improvements feature introduces the following three performance metrics for Context-Based Access Control (CBAC):

- Throughput Improvement—Allows users to dynamically change the size of the session hash table without reloading the router by using the **ip inspect hashtable** command. By increasing the size of the hash table, the number of sessions per hash bucket can be reduced, which improves the throughput performance of the base engine.
- Connections per Second Improvement—Allows only the first packet of any connection to be bumped up to the process switching path while the remaining packets are processed by the base engine in the fast path. Thus, the base engine is no longer slowed down by bumping up several packets or by processing packets twice.
- CPU Utilization Improvement—Allows the CPU utilization of the router running CBAC to be measured while a specific throughput or connections per second metric is maintained. This improvement is used in conjunction with the throughput and connections per second metrics.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftfirewl.htm.

Cisco IOS Telephony Service Version 2.0

The Cisco IOS Telephony Service, under the IP Telephony services umbrella, provides basic Cisco IP phone call-handling capabilities in a LAN environment on the Cisco routers. This feature enables the Cisco multiservice routers to act as the Cisco IOS Telephony Service for the Cisco IP Phone 7960, Cisco IP Phone 7940, Cisco IP Phone 7910, and Cisco IP Conference Station 7935. This feature also helps download phone software images and configures and manages the Cisco IP phones in your LAN. The Cisco IOS Telephony Service provides you with a telephony system perfect for a small office with a small number of extensions.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/access/ip_ph/ip_ks/ipkey2.htm.

Cisco Service Assurance Agent Support for the Cisco 820 Series and SOHO 70 Series

Cisco IOS Release 12.2(8)T adds support for the Cisco Service Assurance Agent feature to Cisco 820 series and Cisco SOHO 70 series routers. For information on configuration for the Cisco Service Assurance Agent, refer to the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf017.htm.

The Cisco 820 series and SOHO 70 series do not currently support the Cisco Service Assurance Agent Application Performance Monitor (APM) feature.

Class-Based Weighted Fair Queueing (CBWFQ)

Class-based weighted fair queueing (CBWFQ) extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, access control lists (ACLs), and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class. A queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class.

CNS Agents SSL Security

CNS Agents SSL Security is a Cisco IOS software feature that allows for the configuration of a secure connection between the CNS Agent, running on the Cisco IOS software-based device, and a CNS Server. Secure Socket Layer (SSL) encryption for CNS connections is enabled on the Cisco IOS device (CNS Agent) side using the **encrypt** keyword with the **cns config initial** or **cns config partial** global configuration mode commands.

CNS Flow-Through Provisioning

The CNS Flow-Through Provisioning feature provides the infrastructure for automated configuration of network devices on a mass scale. Based on the already released 12.2 T CNS event and configuration agents, this extra functionality facilitates the industry's first true "zero-touch" network deployment solution, eliminating the need for the traditional technician truck-roll associated with initial device turn-up. This IOS infrastructure interoperates with CNS IE2100 Intelligent Network Engine, creating the foundation for a closed loop binding of the service provider's operational systems, business systems, and Cisco's order process into a single e-business solution. The result is the first automated work flow ranging from initial subscriber order-entry, through Cisco manufacturing and shipping, to final device provisioning and subscriber billing. This process focuses on a root problem of today's service provider business model—use of human labor in the mass production process of subscriber service activation.

Configurable PSTN Cause Code to SIP Response Mapping

For calls to be established between a Session Initiation Protocol (SIP) network and a Public Switched Telephone Network (PSTN), the two networks must be able to interoperate. One aspect of their interoperation is the mapping of PSTN cause codes, which indicate reasons for PSTN call failure or completion, to SIP status codes or events. The opposite is also true: SIP status codes or events are mapped to PSTN cause codes. Event mapping tables in the document referenced below show the standard or default mappings between SIP and PSTN.

However, you may want to customize the SIP user agent software to override the default mappings between the SIP and PSTN networks. The Configurable PSTN Cause Code to SIP Response Mapping feature allows you to configure specific map settings between the PSTN and SIP networks. Thus, any SIP status code can be mapped to any PSTN cause code, and vice versa. When set, these settings can be stored in NVRAM and are restored automatically on bootup.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmap.htm

Default VPDN Group Template

The Default VPDN Group Template feature introduces the ability to configure global default values for virtual private dialup network (VPDN) parameters in a VPDN template. These global default values are applied to all VPDN groups, unless specific values are configured for individual VPDN groups. Previously, the Cisco IOS software required that VPDN parameters be configured for each individual VPDN group if the system default values were not desired.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdevpdn.htm.

DHCP Client—Dynamic Subnet Allocation API

The DHCP Client–Dynamic Subnet Allocation API feature is an application program interface (API) that is called by the DHCP Server–On-Demand Address Pool Manager feature for obtaining a subnet or releasing a subnet to the source server via DHCP. This feature allows automated configuration of layer 3 devices for simplified deployment.

DHCP Client on WAN Interfaces

The DHCP Client on WAN Interfaces feature extends the Dynamic Host Configuration Protocol (DHCP) to allow PPP over ATM (PPPoA) and certain ATM interfaces to acquire an IP address through DHCP. By using DHCP rather than the IP Control Protocol (IPCP), a DHCP client can acquire other useful information such as DNS server addresses, the DNS default domain name, and default route.

Previously, the **ip address dhcp** interface configuration command could only be used on Ethernet interfaces. This feature allows the **ip address dhcp** command to be used on WAN interfaces.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftwandhp.htm.

DHCP Relay—MPLS VPN Support

The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies. The DHCP relay agent information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent.

In some environments, a relay agent resides in a network element that also has access to one or more Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). A DHCP server that wants to offer service to DHCP clients on those different VPNs needs to know the VPN in which each client resides. The network element that contains the relay agent typically knows about the VPN association of the DHCP client and includes this information in the relay agent information option.

The DHCP Relay–MPLS VPN Support feature allows the relay agent to forward this necessary VPN-related information to the DHCP server using the following three suboptions of the DHCP relay agent information option:

- VPN identifier
- Subnet selection
- Server identifier override

The DHCP Relay–MPLS VPN Support feature enables a network administrator to conserve address space by allowing overlapping addresses. The relay agent can now support multiple clients on different VPNs, and many of these clients from different VPNs can share the same IP address.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdhmpls.htm.

DHCP Server—On-Demand Address Pool Manager

The DHCP Server–On-Demand Address Pool Manager is a feature in which pools of IP addresses can be dynamically increased or reduced in size depending on the address utilization level. This feature supports address assignment using the Dynamic Host Configuration Protocol (DHCP) for customers using private addresses. Each on-demand address pool (ODAP) is configured and associated with a particular Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN).

When configured, the ODAP is populated with one or more subnets leased from a source server and is ready to serve address requests from DHCP clients or from PPP sessions. The source server can be a remote DHCP server or a RADIUS server (via AAA). Currently, only the Cisco Access Registrar RADIUS server supports ODAPs. Subnets can be added to the pool when a certain utilization level (high utilization mark) is achieved. When the utilization level falls below a certain level (low utilization mark), a subnet can be returned to the server from which it was originally leased.

This feature allows customers to optimize their use of IP addresses, thus conserving address space.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftondhcp.htm.

DHCP Server—Option to Ignore All BOOTP Requests

The DHCP Server—Option to Ignore All BOOTP Requests feature introduces the following new global configuration command: **ip dhcp bootp ignore**. This command allows the Cisco IOS DHCP server to ignore received BOOTP requests.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdbootp.htm.

DHCP Server Options Import and Autoconfiguration

The Cisco IOS DHCP server was enhanced to allow configuration information to be updated automatically. Network administrators can configure one or more centralized DHCP servers to update specific DHCP options within the DHCP pools. The remote servers can request or "import" these option parameters from the centralized servers.

This feature was originally introduced in Cisco IOS Release 12.1(2)T. This release is porting the feature into the Cisco 800 series platform.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_dhcpi.htr

Dialer Map VRF-Aware for an MPLS VPN

The Cisco IOS Release 12.2(8)T dialer software is "VRF-aware for an MPLS VPN," which means that it can distinguish between two destinations with the same IP address using information stored in a virtual routing and forwarding instance (VRF). The VRF is identified based on the incoming interface of the packet and is used with a defined destination IP address to determine the telephone number to be dialed.

The Dialer Map VRF-Aware for an MPLS VPN feature allows the dialer software to dial out in a Multiprotocol Label Switching (MPLS)-based Virtual Private Network (VPN). The MPLS VPN model simplifies network routing by allowing several sites to transparently interconnect through the service provider network. One service provider network can support several different IP VPNs, each of which appears to its users as a separate, private network. Within a VPN, each site can send IP packets to any other site in the same VPN because each VPN is associated with one or more VRFs. The VRF is a key element in the VPN technology because it maintains the routing information that defines a customer VPN site.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmapvrf.htm.

Dialer Watch Connect Delay

The Dialer Watch Connect Delay feature introduces the ability to configure a delay in bringing up a secondary link when a primary link that is monitored by Dialer Watch goes down and is removed from the routing table. Previously, the router would instantly dial a secondary route without allowing time for the primary route to come back up. When the Dialer Watch Connect Delay feature is configured, the router will check for availability of the primary link at the end of the specified delay time before dialing the secondary link.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdialwl.htm.

Diff-Serv-aware MPLS Traffic Engineering

MPLS traffic engineering allows constraint-based routing of IP traffic. One of the constraints satisfied by constant bit rate (CBR) is the availability of required bandwidth over a selected path. Diff-Serv-aware Traffic Engineering extends MPLS traffic engineering to enable you to perform constraint-based routing of "guaranteed" traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher quality of service performance (in terms of delay, jitter, or loss) for the guaranteed traffic. Results include virtual leased lines and voice-trunking services.

This release adds support for label-controlled ATM (LC-ATM) interfaces. Previous releases supported Packet-over-SONNET (POS) and ATM permanent virtual circuit (PVC) interfaces.

Disabling V.110 Padding

In networks with devices such as terminal adapters (TAs) and global system for mobile communication (GSM) handsets that do not fully conform to the V.110 modem standard, you will need to disable V.110 padding. To disable the padded V.110 modem speed report required by the V.110 modem standard, use the **no isdn v110 padding** command in interface configuration mode.

DistributedDirector Boomerang Support

Boomerang is a Director Response Protocol (DRP) metric for DistributedDirector. The boomerang server provides a way to select a content server with the fastest response time from a group of redundant content servers. Instead of relying on static maps, boomerang dynamically recognizes problems such as congestion and link failures and avoids them. The content server with the fastest response time, as determined by the priority of the configured metrics, is determined to be the best site.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftddboom.htm

DistributedDirector Cache Auto Refresh

The DistributedDirector Cache Auto Refresh feature works in the background to continuously update all entries in the DistributedDirector cache. When this background refresh feature is initiated, DistributedDirector periodically updates all expired cache entries. The DistributedDirector cache saves the latest answers to all past Domain Name System (DNS) queries that were received since cache auto refresh was initiated, and any repeat request is served directly from the cache when caching is enabled.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftrefrsh.htm.

DistributedDirector Configurable Cache

DistributedDirector maintains an internal cache of entries, which is dynamically configurable. This internal configurable cache consists of sorting events that occur on a per-client basis. Users can configure both the variable size of this internal cache and the amount of time the DistributedDirector system will retain per-client sorting information.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftddcach.htm.

DistributedDirector MIB Support

The Cisco DistributedDirector MIB provides MIB support for DistributedDirector. This MIB contains DistributedDirector statistics, configurations, and status.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftddmib.htm.

Distributed LFI/dQoS over Leased Lines

Note The Distributed LFI/dQoS over Leased Lines feature is also known under the feature title Distributed Link Fragmentation and Interleaving over Leased Lines.

The Distributed LFI/dQoS over Leased Lines feature extends distributed link fragmentation (dLFI) and interleaving functionality on the VIP-enabled Cisco 7500 series routers to leased lines. Previously, Distributed Link Fragmentation and Interleaving was only available for Frame Relay and ATM.

Note Distributed Link Fragmentation and Interleaving for Frame Relay, ATM, and Leased Lines is referred to as dLFI in this feature description.

The dLFI feature supports the transport of real-time traffic, such as voice, and non-real-time traffic, such as data, on lower-speed Frame Relay and ATM virtual circuits (VCs) and on leased lines without causing excessive delay to the real-time traffic.

This feature is implemented using multilink PPP (MLP) over Frame Relay, ATM, and leased lines on VIP-enabled Cisco 7500 series routers. The feature enables delay-sensitive real-time packets and non-real-time packets to share the same link by fragmenting the large data packets into a sequence of smaller data packets (fragments). The fragments are then interleaved with the real-time packets. On the receiving side of the link, the fragments are reassembled and the packet reconstructed.

The dLFI feature is often useful in networks that send real-time traffic using Distributed Low Latency Queueing, such as voice, but have bandwidth problems that delay this real-time traffic due to the transport of large, less time-sensitive data packets. The dLFI feature can be used in these networks to disassemble the large data packets into multiple segments. The real-time traffic packets then can be sent between these segments of the data packets. In this scenario, the real-time traffic does not experience a lengthy delay waiting for the low-priority data packets to traverse the network. The data packets are reassembled at the receiving side of the link, so the data is delivered intact.

The ability to configure Quality of Service (QoS) using the Modular QoS CLI while also using distributed MLP (dMLP) is also introduced as part of the dLFI feature. The ability to configure QoS using the Modular QoS CLI while using dMLP was not supported prior to the introduction of the dLFI feature.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdlfi2.htm.

Distributed Multilink Point-to-Point Protocol

The Distributed Multilink Point-to-Point Protocol (dMLPPP) feature allows you to combine T1/E1 lines in a Versatile Interface Processor (VIP) on a Cisco 7500 series router into a bundle that has the combined bandwidth of multiple T1/E1 lines. This is done by using a VIP MLPPP link. You choose the number of bundles and the number of T1/E1 lines in each bundle. This allows you to increase the bandwidth of your network links beyond that of a single T1/E1 line without having to purchase a T3 line. Non-distributed MLPPP can only perform limited links, with CPU utilization quickly reaching 90% with only a few T1/E1 lines running MLPPP. With distributed MLP, you can increase the router's total capacity. DMLP supports bundling of fractional T1/E1 starting from DS0(64KBps) onwards.

Multiprotocol Label Switching (MPLS) and MPLS-VPN configurations are supported on DMLP bundle interfaces. As of Cisco IOS Release 12.2(8)T, Class-Based Weighted Fair Queueing (CBWFQ) and Low Latency Queueing (LLQ) are supported on DMLP.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/multippp.htm.

DNS Client AAAA Record Lookups over IPv6

The DNS Lookups over an IPv6 Transport feature adds support for IPv6 AAAA record types over an IPv6 transport in the Domain Name System (DNS) name-to-address and address-to-name lookup processes.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/index.htm.

DRP Agent—Boomerang Support

Boomerang is a Director Response Protocol (DRP) metric for DistributedDirector. When the boomerang metric is active, DistributedDirector instructs the DRP to send Domain Name Service (DNS) responses directly back to the querying client. The DNS response contains the addresses of the sites associated with the respective DRP agent. All involved DRPs send back their DNS responses at the same time. The packet of the DRP that is at shortest delay to the client will arrive first. The client may take the first answer and ignore subsequent ones, a standard behavior of all local DNS server implementations. The DRP agent allows configuration for full boomerang support. The boomerang client is the DRP agent.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftdrpcli.htm.

Dual Tone Multifrequency (DTMF) Relay for SIP Calls Using Named Telephone Events

The Dual Tone Multifrequency (DTMF) Relay for SIP Calls Using Named Telephone Events (NTE) feature provides reliable digit relay between Cisco VoIP gateways when a low bandwidth codec is used. Using NTE to relay DTMF tones provides a standardized means of transporting DTMF tones in Real-Time Transport Protocol (RTP) packets. This feature also adds SIP phone support.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ft_dtmf.htm.

Easy VPN Server

The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x software clients and Cisco VPN hardware clients. It allows a remote end user to communicate using IP Security (IPSec) with any Cisco IOS Virtual Private Network (VPN) gateway. Centrally managed IPSec policies are "pushed" to the client by the server, minimizing configuration by the end user.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftunity.htm.

Enabling Fax Rate on POTS to POTS Fax Calls

This command line interface (CLI) change was made to enable a fax relay between two plain old telephone service (POTS) dial peers to cover the case in which a fax call fails if it is made without DSP (digital signal processor) involvement.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftfxpots.htm.

Encrypted Vendor-Specific Attributes

The Encrypted Vendor-Specific Attributes feature introduces support for the following three types of string vendor-specific attributes (VSAs):

- Tagged string VSA—To retrieve the right value for this VSA, the Tag field must be parsed correctly. The value for this field can range only from 0x01 through 0x1F. If the value is not within the specified range, the RADIUS server will ignore the value and consider the Tag field to be a part of the attribute string field.
- Encrypted string VSA—This VSA has a Salt field that ensures the uniqueness of the encryption key that is used to encrypt each instance of the VSA. The first and most significant bit of the Salt field must be set to 1.
- Tagged and Encrypted string VSA—This VSA is similar to encrypted string VSAs *except* this VSA has an additional Tag field. If the Tag field is not within the valid range (0x01 0x01 through 0x1F), it is considered to be part of the Salt field.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftencvsa.htm.

Enhanced Billing Support for SIP Gateways

The Enhanced Billing Support for SIP Gateways feature describes the changes to authentication, authorization, and accounting (AAA) records and the RADIUS implementations on Cisco Session Initiation Protocol (SIP) gateways. These changes were introduced to provide customers and partners with the ability to effectively bill for traffic transported over SIP networks.

Username Attribute

The username attribute is included in all AAA records and is the primary means for the billing system to identify an end user. The password attribute is included in authentication and authorization messages of inbound Voice over IP (VoIP) call legs.

For most implementations, the SIP gateway populates the username attribute in the SIP INVITE request with the calling number from the FROM: header and the password attribute with null or with data from an Interactive Voice Response (IVR) script. If a Proxy-Authorization header exists, it is ignored. A new Cisco IOS command, **aaa username**, determines the information with which to populate the username attribute.

Within the Microsoft Passport authentication service that authenticates and identifies users, the passport user ID (PUID) is used. The PUID and a password are passed from a Microsoft network to the Internet telephony service provider (ITSP) network in the Proxy-Authorization header of a SIP INVITE request as a single, base-64 encoded string. For example,

```
Proxy-Authorization: basic MDAwMzAwMDA4MDM5MzJlNjou
```

The new Cisco IOS **aaa username** command enables parsing of the Proxy-Authorization header; decoding of the PUID and password; and populating the PUID into the username attribute and the decoded password into the password attribute. The decoded password is generally a "." because a Microsoft Network (MSN) authenticates users prior to this point. For example,

```
Username = "123456789012345"
Password = "Z\335\304\326KU\037\301\261\326GS\255\242\002\202"
```

The password in the example above is an encrypted "." and is the same for all users.

SIP Call ID

From the Call ID header of the SIP INVITE request, the SIP Call ID is extracted and populated in a Cisco vendor-specific attribute (VSA) as a new attribute-value pair *call-id=string*. The attribute-value pair can be used to correlate RADIUS records from Cisco Session Initiation Protocol (SIP) gateways with RADIUS records from other SIP network elements, for example, proxies. For complete information on this attribute-value pair, refer to the *RADIUS Vendor-Specific Attributes Voice Implementation Guide*.

Session Protocol

Session Protocol is another new attribute-value pair that indicates if the call is using Session Initiation Protocol (SIP) or H.323 as the signaling protocol. For complete information on this attribute-value pair, refer to the *RADIUS Vendor-Specific Attributes Voice Implementation Guide*.

Silent Authentication Script

As part of the Enhanced Billing Support for SIP Gateways feature, a new Tool Command Language (TCL) Interactive Voice Response (IVR) API 2.0 Silent Authorization script has been developed. The Silent Authorization script allows users to be authorized without having to separately enter a username or password into the system. The script automatically extracts the passport user ID (PUID) and password from the SIP INVITE request and then authenticates that information through RADIUS authentication and authorization records. The script is referred to as silent because neither the caller nor the called party hears any prompts.

Further Documentation

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftmsnbil.htm.

Enhanced Password Security

The Enhanced Password Security feature allows you to configure Message Digest 5 (MD5) encryption for username passwords. Before the introduction of this feature, there were two types of passwords associated with usernames: Type 0, which is a clear text password visible to any user who has access to privileged mode on the router, and type 7, which is a password with a weak, exclusive, or type encryption. Type 7 passwords can be retrieved from the encrypted text by using publicly available tools.

Use the **username secret** command to configure a username and an associated MD5-encrypted secret.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_md5.htm.

Error Log Count Enhancement

The Cisco IOS logging facility allows you to save error messages locally or to a remote host. When these error messages exceed the capacity of the local buffer dedicated to storing them, the oldest messages are removed. To provide you with more information about messages that have occurred and may have been removed from the local buffer, an error log counter tabulates the occurrences of each error message and time-stamps the most recent occurrence.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fterrlog.htm.

Event Tracer

The Event Tracer feature provides a binary trace facility for troubleshooting Cisco IOS software. This feature gives Cisco service representatives additional insight into the operation of the Cisco IOS software and can be useful in helping to diagnose problems in the unlikely event of an operating system malfunction or, in the case of redundant systems, route processor switchover.

This feature was originally introduced in Cisco IOS Release 12.0(18)S.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s18/evnttrcr.htm.

Fax Detection for Cisco 2600 Series and Cisco 3600 Series Routers

Note The Fax Detection for Cisco 2600 Series and Cisco 3600 Series Routers feature is also known under the feature title Fax Detection (Single-number Voice and Fax).

On Cisco 2600 series and Cisco 3600 series routers equipped with digital and analog voice network modules, the fax detection feature enables service providers to deploy unified communications, in which each subscriber has a single E.164 number for both voice and fax by providing the capability to detect automatically whether an incoming call is voice or fax. Supported network modules are NM-HDV with voice interface cards (VIC)/voice WAN interface cards (VWIC) for digital T1connections and Voice 2V with VIC FXS for analog connections. VWIC and VIC FXS are the voice interface cards within the network modules. When configured for fax detection, the gateway automatically listens to incoming calls to discriminate between voice and fax. The gateway then routes the calls to the appropriate application or server.

Note The fax detection feature requires the Cisco 2600 series and Cisco 3600 series routers to have a minimum of 128MB RAM.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/pull2snf.htm.

Firewall Feature Set

The Cisco IOS Firewall feature set provides firewall-specific security features to the Cisco CVA122 Cable Voice Adapter. When this feature is enabled, the router acts as a buffer between the Internet and other public networks and the private network that is connected to the router. Security is provided by access lists, as well as by examining incoming traffic for suspicious activity.

The firewall-specific security features include the following:

- Authentication proxy services to intelligently apply specific security policies on a per-user basis without impacting performance.
- Checking packet headers and dropping suspicious packets to detect and prevent denial of service attacks, such as ICMP and UDP echo packet flooding, SYN packet flooding, half-open or other unusual TCP connections, and deliberate misfragmentation of IP packets.
- Context-Based Access Control (CBAC) which gives internal-to-the-firewall users secure, per-application-based traffic control across the Internet/Intranet. This includes protection against Simple Mail Transfer Protocol (SMTP) attacks, one of the most common attacks against computers connected to the Internet.
- Dynamic port mapping to allow network applications with well-known port assignments to use customized port numbers. This mapping can be done on a host-by-host basis or for an entire subnet, providing a large degree of control over which users can access different applications.
- Intrusion Detection System (IDS) that recognizes the signatures of the most common attack profiles. When an intrusion is detected, IDS can perform a number of actions: send an alarm to a syslog server or to NetRanger Director, drop the packet, or reset the TCP connection.
- Java blocking to protect against destructive Java applets. Applets can be allowed only from known and trusted sources or blocked completely.
- Real-time and configurable alerts and audit trail capabilities to record and time-stamp source and destination hosts.
- Support for a broad range of commonly used protocols, including H.323 and NetMeeting, FTP, HTTP, MS Netshow, RPC, SMTP, SQL*Net, and TFTP.
- User-configurable audit rules, real-time alerts, and audit-trail logs.

Gatekeeper Transaction Message Protocol Interface Resiliency Enhancement

Gatekeeper Transaction Message Protocol (GKTMP) is used between the Cisco IOS Gatekeeper and a server to provide enhanced call routing and address translation services. The GKTMP Interface Resiliency Enhancement feature adds additional parameters in the disengage request (REQUEST DRQ) message sent from the gatekeeper (GK) to the server. It also provides new request alive (REQUEST ALV) and response alive (RESPONSE ALV) messages between the gatekeeper and server, server failure detection, and a flow control command.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122x/122xb/122xb_2/ftgkire.htm.

Generic Routing Encapsulation (GRE) Tunnel Keepalive

The GRE Tunnel Keepalive feature provides the capability of configuring keepalive packets to be sent over IP-encapsulated generic routing encapsulation (GRE) tunnels. You can specify the rate at which keepalives will be sent and the number of times that a device will continue to send keepalive packets without a response before the interface becomes inactive.

Refer to the following document for additional information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/grekpliv.htm.

GKTMP Security Token Enhancement

The GKTMP Security Token Enhancement feature provides support for ClearTokens in messages between a NetSpeak route server and the Cisco IOS gatekeeper. The Request ARQ, Response ARQ, Response ACF, Request LRQ, Response LRQ, Request LCF, and Response LCF messages between the Cisco IOS gatekeeper and the route server now include ClearTokens. In addition, the Response ARQ messages include both gateways in a local domain or zone and remote zone gatekeepers and allow prioritization of the resulting sets of gateways. The Response LRQ messages support a combination of endpoint addresses and a list of remote zone gatekeepers to which to forward the LRQ message.

G.SHDSL Symmetric DSL Support

G.SHDSL is a new multirate symmetric high-speed digital subscriber line (DSL) technology for the local loop that connects customer premises equipment (CPE) to the central office (CO) in the access network. This access technology for business applications is important because of its symmetric and multirate functionality. G.SHDSL refers to the approved standard officially designated in International Telecommunication Union-Telecommunications Standards Section (ITU-T) G.991.2.

IGMP Version 3—Explicit Tracking of Hosts, Groups, and Channels

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to neighboring multicast routers. IGMP is available in Versions 1, 2, and 3. IGMP Version 3 (IGMPv3) is supported in Cisco IOS Release 12.0(15)S, 12.1(5)T, 12.1(8)E, and later releases.

The IGMP Version 3—Explicit Tracking of Hosts, Groups, and Channels feature enables a multicast router to explicitly track the membership of all multicast hosts in a particular multiaccess network. This enhancement to the Cisco IOS implementation of IGMPv3 enables the router to keep track of each

CPL/AC

PREGÃO
050/2003

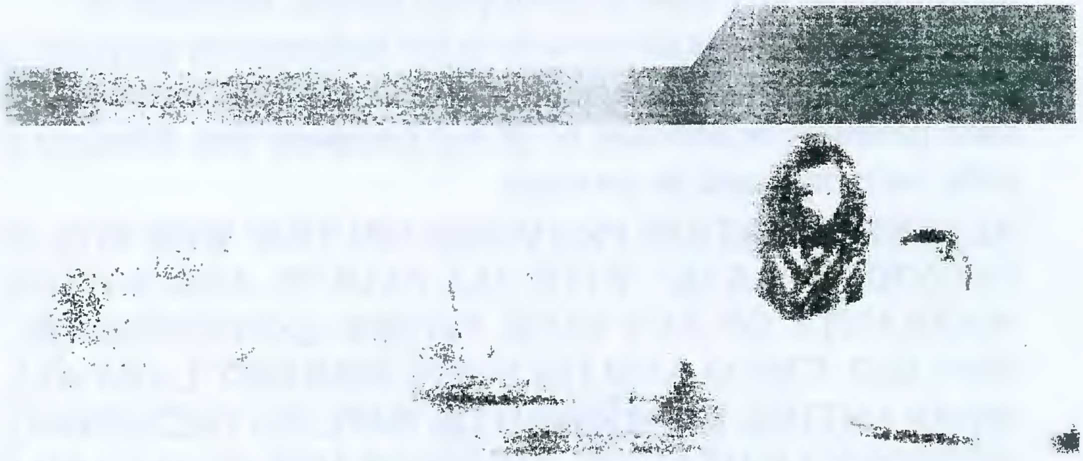
LOCAÇÃO DE
EQUIPAMENTOS
DE INFORMÁTICA
INCLUINDO
ASSISTÊNCIA
TÉCNICA E
TREINAMENTO

HP INVENT –
MANUAL
APÊNDICES GA A
GQ

2003
PASTA 12

Ap. GA

CISCO SYSTEMS



Cisco Products Quick Reference Guide

April 2003

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-785983
Text Part Number: 78-5983-11

General Disclaimer

Although Cisco has attempted to provide accurate information in this Guide, Cisco assumes no responsibility for the accuracy of the information. Cisco may change the programs or products mentioned at any time without prior notice. Mention of non-Cisco products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

ALL INFORMATION PROVIDED ON THIS WEB SITE IS PROVIDED “AS IS,” WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

CISCO AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS OR SERVICES, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF THE GUIDE OR ANY CISCO PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Many of the Cisco products and services identified in this Guide are provided with written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this Guide shall be deemed to expand, alter, or modify any warranty or license provided by Cisco with any Cisco product, or to create any new or additional warranties or licenses.

CONTENTS

Introduction

CHAPTER 1 Routers

CHAPTER 7 Broadband and Dial Access Products

Introduction

Cisco Products Quick Reference Guide (CPQRG)

CPQRG Background

The Cisco Products Quick Reference Guide (CPQRG) is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many of Cisco's products. The CPQRG is primarily published to support Cisco partners, resellers, sales account teams, and even end-user customers who need a broad, high-level overview of Cisco products, but at that moment do not have access to Cisco's Web site, the Cisco Connection Online (CCO) at **http://www.cisco.com**.

Because this book is only published twice per year, there are likely to be new products, configurations, and part numbers not included in this edition. Note: For the most up-to-date and comprehensive information about Cisco products and solutions, please refer to our on-line information or consult a Cisco representative.

CPQRG Ordering Information

Additional printed copies of this book can be purchased on an as-needed basis or through an annual subscription. To order, see **http://shop.cisco.com/login**.

For questions regarding the CPQRG ordering process, please send an email to **companystore@external.cisco.com**.

For questions, comments or to download an Adobe PDF version of the CPQRG, go to **http://www.cisco.com/go/guide**.

How to Get More Complete Product Information

Cisco Product Catalog	For more comprehensive information on all of Cisco's products, please refer to the Cisco Product Catalog at: http://www.cisco.com/univercd/cc/td/doc/pcat/
Cisco Connection Online (CCO)	For even more complete product and solution information, please go to CCO at http://www.cisco.com. In addition to product, technology, and network solutions support, CCO provides a wealth of information including how to find an authorized representative or partner, how to order products, technical support/customer service, Cisco Corporate news and information, and links to training/events/seminars.

Cisco Systems Overview

Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Cisco's Internet Protocol-based (IP) networking solutions are the foundation of the Internet and most corporate, education, and government networks around the world. Cisco provides the broadest line of solutions for transporting data, voice and video within buildings, across campuses, or around the world.

Today, the Internet and computer networking are an essential part of business, learning and personal communications and entertainment. Virtually all messages or transactions passing over the Internet are carried quickly and securely through Cisco equipment. Cisco solutions ensure that networks both public and private operate with maximum performance, security, and flexibility. In addition, Cisco solutions are the basis for most large, complex networks used by corporations, public institutions, telecommunication companies, and are found in a growing number of medium-sized commercial enterprises.

Cisco was founded in 1984 by a group of computer scientists from Stanford University. Since the company's inception, Cisco engineers have been prominent in advancing the development of IP- the basic language to communicate over the Internet and in private networks. The company's tradition of innovation continues today with Cisco creating leading products and key technologies that will make the Internet more useful and dynamic in the years ahead. These technologies include: advanced routing and switching, voice and video over IP, optical networking, wireless, storage networking, security, broadband, and content networking.

In addition to technology and product leadership, Cisco is recognized as an innovator in how business is conducted. The company has been a pioneer in using the Internet to provide customer support, sell products, offer training, and manage finances. Drawing upon the company's own Internet best practices and core-value of customer focus, Cisco has established the Internet Business Solutions Group (IBSG) dedicated to helping top business leaders transform their own businesses into e-businesses.

As a company, Cisco operates on core values of customer focus and corporate citizenship. The company's philanthropic efforts are committed to helping communities prosper while also encouraging Cisco employees to learn about the needs of the communities where Cisco operates. Also, to help bolster education around the world, the company has founded Cisco Networking Academies in 128 countries dedicated to teaching students to design, build, and maintain computer networks.

Cisco Channel Partner Program

Whether you provide services, solutions or a combination of both, Cisco is committed to your success. The Cisco Channel Partner Program can help partners create a sustainable business model in a fast-changing environment, where customers require value-added services, focused technical expertise, and higher levels of satisfaction. As a Cisco certified partner, you'll have the backing of the Cisco brand, and access to world-class products and service packages, technical support, productivity tools, online training, marketing resources and sales promotions.

The Partner Program integrates the technology focus of each Cisco Partner Specialization, flexible individual career certification requirements, customer satisfaction targets, and pre- and post-sales support capabilities. These elements make up the points-based structure of the overall program requirements. There are three partner certification levels: Gold Certification, Silver Certification, and Premier Certification.

The Partner Program requires every partner to specialize in technology areas as part of the program requirement. You may choose the technology area for Specialization, but must earn a minimum number of Specialization points to become certified. You may decide to be strictly a specialized partner or specialize your organization as a means to achieving certification. Either way, you'll have access to structured training roadmaps, free online technical and sales education and video-on-demand content to build your knowledge and skill level through the Partner E-Learning Connection **http://cisco.partnerelearning.com**

For More Information

See the Channel Partner Program Web Site: **http://www.cisco.com/go/channelprograms**

If you are interested in reselling Cisco product without becoming certified or specialized, see **http://www.cisco.com/go/reseller**

Reseller and Customer Support

Reseller Sales and Technical Assistance Contact Information

Customer Help Lines	Contact Information
US Distribution Presales Helplines[1]	Comstor: 800-COMSTOR, option 3 Ingram Micro: 800-445-5066, enter Ingram customer #, dial extension 24041 Tech Data: 800-237-8931, extension 77776
Presales—Partner/Reseller Helpline	800 553-6387 (within U.S.) 408 526-7208 (outside U.S.) http://CiscoPartner.custhelp.com/
Post-Sales—Technical Assistance Center (TAC)	800 553-6387 (within U.S.) 408 526-7209 (outside U.S.) tac@cisco.com (e-mail)

[1] Follow voice prompts to access: Pre-sales Assistance of Network Validation & Product Information, Reseller Support, Customer Service, Service Contract Sales, Reporting a technical problem/open a trouble ticket, and Seminars, Events, Training & Certification

Helpful Cisco Web Sites

Cisco Web Site	URL[1]
Worldwide Contacts Cisco office locations; directions; maps; and sales, partners, and channel contacts.	http://www.cisco.com/go/wwcontacts
Partner Relationship Central Find a Channel Account Manager (CAM), Distributor, apply to the Cisco Channel Partner Program, or update your profile.	http://www.cisco.com/go/prc
Technical Support For customer support tips, software center, online documents, and more.	http://www.cisco.com/go/support http://www.cisco.com/public/Tech_support.shtml http://www.cisco.com/public/technotes/serv_tips.shtml
Cisco Products Quick Reference Guide This guide is available on line (in PDF and HTML); it is continually updated between bi-yearly printings. CCO login required.	http://www.cisco.com/go/guide
Cisco Subscription Service Ordering service for one-time purchase of or annual subscriptions to this guide or other Cisco documents and CDs; order online, or order by phone by calling 800 768-7162 (U.S. or Canada) or 925 327-4072 (outside the U.S.).	http://shop.ciscocom/login
Partner Help Search partners' frequently asked questions and ask for the help you need	http://ciscopartnercusthelp.com/
Certification/Specialization Application Apply for a Cisco Certification or Specialization	http://www.cisco.com/warp/customer/765/partner_programs/apply/
Find a Channel Account Manager Search for the Cisco Channel Account Manager assigned to your company	http://tools.cisco.com/WWChannels/CAMLOC/jsp/cam_locator.jsp
Partner Registration Begin your relationship with Cisco by registering as a Cisco Registered or Certified Partner	http://tools.cisco.com/WWChannels/GETLOG/jsp/GetLoginjsp?page=PartnerUserHomePage
Tool Index	http://www.cisco.com/en/US/partners/partners_tool_index.html
Get CCO Access Register for a guest-level Cisco.com ID as a prerequisite for partner level access	http://tools.cisco.com/RPF/register/register.do
Associate Myself With A Partner If you are an employee of Cisco Registered and Cisco Certified or Specialized Partners, you can associate yourself with your company and upgrade your current Cisco.com ID to partner level	http://tools.cisco.com/WWChannels/GETLOG/jsp/GetLoginjsp?page=PartnerUserHomePage
Partner Self Service Use this suite of tools to manage personal and company information in the Cisco partner database	http://tools.cisco.com/WWChannels/GETLOG/welcome.do
Update Company Data If you are a registered partner administrator, you can update company and contact information	http://www.cisco.com/warp/public/765/tools/certification/
Worldwide Distributors Web Site List, by country, of authorized Cisco Distributors who stock and resell Cisco products.	http://www.cisco.com/go/disti
Distribution Product Reference Guide (DPRG) Complete list of pricing information, part numbers, and more for distribution (2-tier) products. Data is refreshed nightly. CCO login required.	http://www.cisco.com/dprg
Partner Business Central—Browse and Configure Products An ecommerce web site with a configuration tool to validate channel product options; also select and compare products, check price and availability, and submit your order to your distributor online. CCO login required—click on "Browse and Configure Products".	http://www.cisco.com/go/partner/bizcentral
End-of-Life Matrix Last order and end-of-life dates for Cisco products	http://www.cisco.com/go/eol
Training Cisco University—Offers detailed course material on the latest technical topics throughout the year targeted for Resellers, Partners and Cisco Sales representatives. Also see the Partner E-Learning Connection.	http://www.cisco.com/go/ciscou http://cisco.partnerelearning.com

1. Additional CCO access required for most URLs.

Partner and Reseller Service and Support Offerings

Various partner and reseller service and support programs are available according to certification level and method of purchase from Cisco:

Method of Purchase	Service and Support Offerings
Direct from Cisco (only available to Partners with Direct contracts)	• *System Integrator Support*—System Integrator Support 98 (SIS98) program is designed for Silver and Gold partners who wish to provide their own brand of support to their end customers with back-end support from Cisco – SMARTspares provides partners using SIS98 the opportunty to leverage Cisco's logistics infrastructure to provide their customers with enhanced delivery services. • *Shared Support*—Currently only available in the US, Cisco's Shared Support program is designed for Silver and Gold partners who wish to provide their own brand of support to their end customers while leveraging Cisco's Technical Assistance Center (TAC) and logistics infrastructure • *Cisco Brand Resale*—Program allows partners to provide Cisco's services (SMARTnet, etc.) directly to their end customers
2-Tier (through a Distributor)	• *Packaged Services*—Partners and Resellers may purchase warranty extension, hardware replacement, installation and configuration, technical support, software upgrades, and online services. Several of these services have been bundled together to offer convenient service solutions for Cisco customers.

Packaged Resalable Service Products (only via Distributors/2-Tier):

Product	Description
Maintenance Services	
SMARTnet Maintenance	Provides customers with software maintenance, registered access to CCO, advance replacement of hardware, and technical support required for self-maintenance. SMARTnet maintenance has three delivery options: • SMARTnet 8x5xNBD (Next Business Day)—8 hours/day, 5 days/week, next-business-day hardware replacement • SMARTnet 8x5x4—8 hours/day, 5 days/week, 4-hour hardware replacement • SMARTnet 24x7x4—24 hours/day, 7 days/week, 4-hour hardware replacement Available through resellers and distributors.
SMARTnet Onsite	Provides all the benefits of SMARTnet maintenance, plus one of the following onsite hardware services for repairs: • SMARTnet Onsite 8x5xNBD—8 hours/day, 5 days/week, next-business-day response • SMARTnet Onsite 8x5x4—8 hours/day, 5 days/week, 4-hour response • SMARTnet Onsite 24x7x4—24 hours/day, 7 days/week, 4-hour response Packaged SMARTnet OnSite 24x7x4 provides SMARTnet OnSite 24x7x4 service in a shrink-wrapped package, allowing it to be effectively marketed through resellers.
Cisco Advance Replacement	Advance Replacement offers customers the flexibility to cover their equipment with an advance replacement service only. Cisco Advance Replacement comes with a full year of advance replacement coverage, guest access to the public portion of Cisco Connection Online (CCO), and a single technical support incident. This service is intended to be used by customers who need to supplement service offered by their reseller with a replacement option from Cisco.
Software Application Support plus Upgrades (SASU)	Software Application Support plus Upgrades provides customers with software upgrades and maintenance releases for Cisco Application Software, registered access to Cisco.com plus technical support, for one year. For when a customer needs investment protection on software purchases and/or access to the latest software while eliminating unexpected budget revisions.
Noncontract and Consulting Services	Cisco provides noncontract services at current time-and-materials rates. For more information contact Customer Services at 1-800-553-NETS or 1-415-326-1941.
Startup Services	
Total Implementation Services (TIS)	Cisco Total Implementation Solutions (TIS) is a portfolio of services that deliver the tools, expertise, and resources needed to install, configure, and implement Cisco equipment. TIS is intended to supplement services that resellers provide, either directly or indirectly, to their customers. Product Components: Installation, Configuration, and Implementation. For more information, see http://www.cisco.com/go/tis

For More Information

See the Partner and Reseller Support Services Web page at: **http://www.cisco.com/en/US/products/index.html** (CCO login required)

Product Warranty Information

All Cisco hardware and software products are covered for a minimum of 90 days. Some products have a longer or more appropriate coverage, ranging from One-Year to Limited Lifetime warranties. Note that all Warranties are applicable to original owner only and support is subject to product end-of-life terms.

Warranty[1]	Entitlements Description
Cisco Standard 90-day Hardware Warranty, Software Warranty and License Agreement (78-5235-vvrr)	• Advance Replacement shippingwithin 10 business days from RMA date, within 90 days of original shipment from Cisco or from Cisco Reseller • 90-Day Assurance thatthe Media SW is delivered is defect-freeandthe SW conformsto its published specifications • Guest Access to Cisco Connection Online (CCO)
90-Day Limited Hardware Warranty(78-5236-vvrr)	• Advance Replacement shippingwithin 10 business days from RMA date, within 90 days of original shipment from Cisco or from Cisco Reseller • 90-Day Assurance thatthe Media SW is delivered is defect-freeandthe SW conformsto its published specifications • Guest Access to Cisco Connection Online (CCO)
One-Year Limited Hardware Warranty (78-10747-vvrr)	• Advance Replacement shippingwithin 10 business days from RMA date withinOne Year of original shipment from Cisco or from Cisco Reseller • 90-Day Assurance thatthe Media SW is delivered is defect-freeandthe SW conformsto its published specifications • Guest Access to Cisco Connection Online (CCO)
Limited Lifetime Hardware Warranty (78-6310-vvrr)	• Advance Replacement shippingwithin 10 business days from RMA date during supported life of the product,startingoriginal ship date from Ciscoor Ciscoreseller. (fanand power supplywarranty limited to 5 years from ship-date) • 90-Day Assurance thatthe Media SW is delivered is defect-freeandthe SW conformsto its published specifications • Guest Access to Cisco Connection Online (CCO)
End-User Software License Agreement and Software Warranty (78-3621-vvrr)	• 90-Day Assurance thatthe Media SW is delivered is defect-freeandthe SW conformsto its published specifications • End User License Agreement terms • Guest Access to Cisco Connection Online (CCO)
5-Years Limited Hardware and 1-Year Limited Software Warranty (78-13712-vvrr)	• Replacementshipping within 15 business days from RTF date within 5 years from the original ship date from Cisco or Cisco reseller • One-Year SW support includes availability of bug fixes and maintenance releases • Cisco TAC 24x7 support for P1/P2 cases for Five years • Guest Access to Cisco Connection Online (CCO)

[1] "vv" and "rr" suffixes of the warranty document numbers represent the revision and version numbers respectively.

For More Information

See the Web site:
http://www.cisco.com/en/US/products/prod_warranties_listing.html

Cisco Capital Financing

Cisco Systems Capital cffers a variety of financing and equipment leasing alternatives, both short term and long term, to customers and partners in the United States, Canada, Europe, Asia, Australia, and Latin America. Cisco Capital's financial solutions offer customers the ability to acquire new technologies or refresh existing equipment through flexible, easy-to-use programs.

For More Information

See the Cisco Systems Capital Web site: **http://www.cisco.com/go/CiscoCapital**
Within the United States, call 800 730-4090.

Cisco Authorized Refurbished Equipment (US and Canada Only)

Customers looking for used Cisco equipment can now be assured of the quality and support they come to expect from new Cisco products, through the Cisco Authorized Refurbished Equipment program. Cisco Authorized Refurbished Equipment gives customers a price competitive alternative to buying uncertified and unlicensed products off the secondary market. All equipment sold through this program is labeled "Refurbished by Cisco Systems," indicating that the product is Cisco tested, refurbished, authorized, and supported. The program is limited to certain countries, so interested customers should check with their local Cisco account manager of Cisco authorized reseller for availability.

For More Information

End Users/Customers:
cisco.com/en/US/ordering/or6/or17/order_refurbished_equipment_program_description.html
Resellers: **http://www.cisco.com/go/refurb** (click on "Refurbished Products")

Cisco Services

Cisco Services offers a wide range of services and support to customers, partners and resellers. Through a suite of support services Cisco enables you to improve the overall efficiency of your network operations and network performance, while benefiting from the broad range of Cisco engineering knowledge and experience base, leading practices and innovative, web-based tools.

Cisco Advanced Services (AS) is a comprehensive suite of professional engineering support offerings of Cisco networking solutions delivering the highest levels of availability, quality of service, and security for your specific network needs to realize business return on investment through high performance networking and communications applications enablement. Cisco Technical Support Services (TSS) offer leading-edge services to improve customer productivity, protect customer investment, and maximize operational efficiency. Cisco TSS solutions provide access to highly skilled engineers with technical expertise on multiple disciplines of technology. In addition, Cisco TSS provides you with the online tools and resources, software support and hardware replacement options to address your challenges and provide rapid problem resolution. Key support tools and knowledge provide your staff with the ability to avoid problems, maximize network utility, and expedite problem resolution.

For More Information

Technical Support Services:
http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/serv_group_home.html
Advanced Services:
http://www.cisco.com/en/US/products/svcs/ps11/serv_category_home.html

CHAPTER 1

Routers

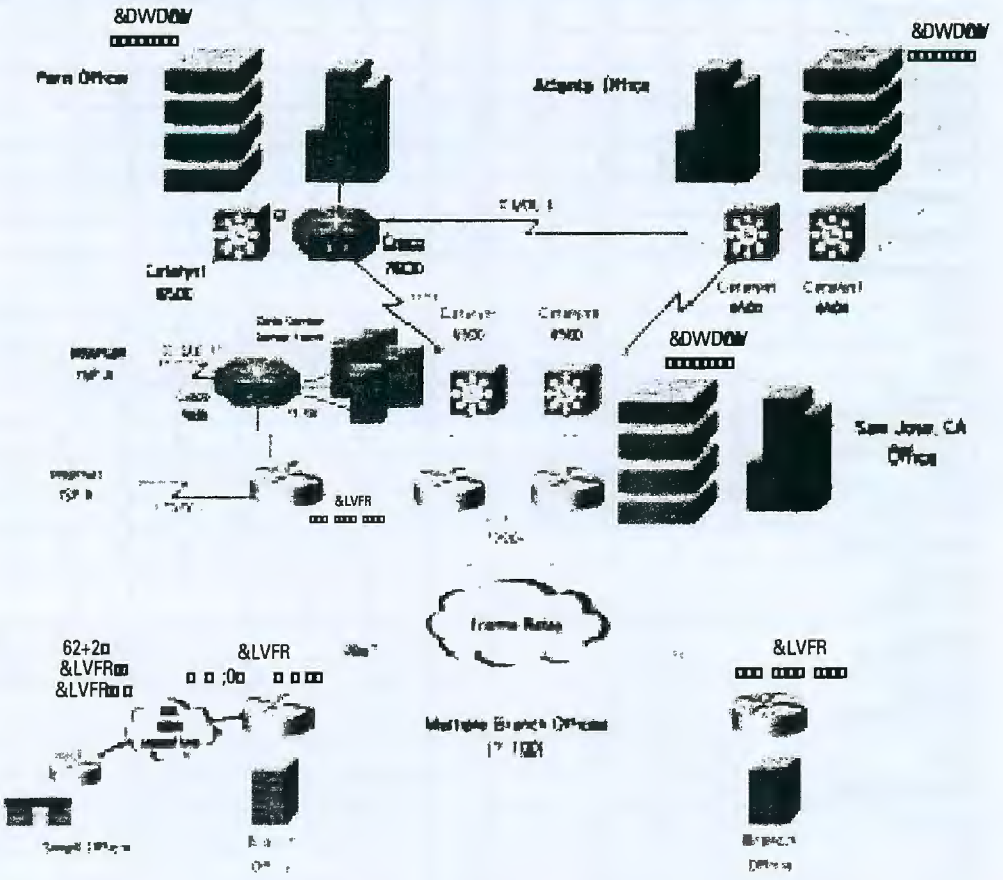
Routers at a Glance

Product	Features	Page
Cisco IOS® Software	See the Chapter 9—CiscoIOS Software and Network Management foran overview of Cisco IOS Software	9-4
Cisco SOHO Series Secure Broadband Routers	Ethernet, ADSL, ADSL over ISDN, and G.SHDSL Routers for Small Office andHome Ofices • Integrated securty of Cisco IOS Software with Stateful Inspection Frewall and software-based 3DES encryption • Easy setup and deployment usng Cisco Router Web Set Up Tool (CRWS) • Offers many local and remote debug and troubleshooting features in Cisco IOS Software	1-8
Cisco 800 Series Router	Ethernet, ADSL,ADSL over ISDN, G.SHDSL, ISDN, and serial routers for small remote offices and teleworkers • 1-port Ethernet, 1-port ADSL, ADSL over ISDN or G.SHDSL or 1-port BRI (optional NT1), 1-port serial WAN • 4-port Ethernet hub or 10/100 swithch on most models and 2 analog telephone ports on ISDN models and 4 analog voice ports on 827-4V • Advanced securty features including statefulinspectionfirewall and hardware assisted encryption (830 series) • Toll quality voice with VoIP (Cisco 827-4V) • Dial back up and out-of-band management (Cisco 830 series)	1-9
Cisco 1700 Series Router	Flexible, secure, modular access routers • 1-port autosensing 10/100 Fast Ethernet LAN • Modular slots support a wide variety of WAN and voice interface cards • Supports secure Internet, intranet,and extranet access as well as new WAN applications including VPNs, integrated voice/data (VoIP), and broadband services • VLAN Capability • Supports upto three Ethernet connectionswith 1 FE and 2 ENET WICs	1-11
Cisco 2500 Series Router	Fixed-port configuration accessservers • The Cisco AS2509-RJ/AS2511-RJ access/terminal servers provide Ethernet LAN connectivity and enable 8 or 16 (respectively) users/devices via async connections • Ideal for low-density analog telephone lne dial access applications via external modems	1-14
Cisco 2600 Series Router	Modular multiservice router • Single or dual LAN (Ethernet, 10/100 Mbps Ethernet, Token Ring and mixed Ethernet options) • Wide variety of interface support, including integrated 16-port switching, high-density analog and digital, voice, Cisco IOS Firewall and VPN, async and sync serial, ISDN, Fractional and channelized T1/E1, Ethemet, analog modems, ADSL, G.SHDSL, switching integration, and ATM support • Shares WAN interface cards and network modules with Cisco 1700, 3600 and 3700 series • Cisco 2610XM, 2620XM, and 2650XM models offer the features of Cisco 2600 with more default memory, capacity, performance and FE support on all models.	1-16
Cisco 3600 Series Router	Modular multiservice high-density access router • 2-, 4-, and 6-slot models • Wide variety of media support including: high density analog and digital voice, Cisco IOS Firewall and VPN, integrated 16-port switching, ADSL, and G.SHDSL, async and sync serial, BRI and PRI ISDN, channelized T1/E1, Ethernet, Fast Ethernet, Token Ring, digital and analog modems, and ATM • Digital and analog voice/fax over IP or Frame Relay or ATM • The Cisco 3640 is no longer orderable. Customers are encouraged to migrate to the Cisco 3700 Series Routers. On an interim basis we have made available the Cisco3640A as an alternative for customers with configurations not available on the Cisco3700.	1-22

Product	Features	Page
Cisco 3700 Series Router	Modular multiservice high-density access router • Enable higher levels of application andservice integration inenterprise branch offices in a small form factor – Supportsintegrated firewall, intrusion detection, and VPN capabilities and offloads processing to on-board AdvancedIntegration Module (AIM) – Combinesflexible routing and lowdensity switching in a single platformwith new 16 and 36-port EtherSwitch module – Delivers internalin-line powerfor the EtherSwitch portsfor a single platform Branch Office IP Telephony and Voice Gateway – Conserves WAN bandwidth with Content Enginemodule to combine intellgent caching, content routing and management – Higher performanceenables scalable deployment of multiple, concurrent applications • Wide variety of interface support, including integrated36 and 16-port switching, high-density analog anddigital, voice, Cisco IOS Frewall/IDS and VPN, Fractional and channelizedT1/E1 and DS-3, Ethernet, Gigabit Ethernet and ADSL. • Shares WAN interface cardsand networkmodules with Cisco 1700, 2600/2600XM, and 3600 series	1-26
Cisco 7100 Series VPN Router	Large branch and centralsite VPN router, for a dedicated site-to-site VPN solution See Chapter 5—VPN and Security for information onthe Cisco 7100 Series VPN Routers	5-11
Cisco 7200 Series Router	WAN-edge router providing intelligentservices, modularity, high performance, investment protection, and scalability in a small form factor • Modular 3 RU Chassis • 4- or 6-slot modelsand choice of system processors for up to 1 Mpps performance • Wide variety of LAN and WAN options, including Ethernet,Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, serial, ISDN, HSSI, ATM, Packet over SONET, DPT/RPR	1-31
Cisco 7300 Series	Network Edge routerwith high perfomance IP services delivered at optical speedsfor service providers and enterprise networks • Compact and modular 4 rack unit chassis—4 slots • High performance connectivity—T3 through OC48/STM16 with 3.5 Mpps performance • Built-in Gigabit Ethernet connectivity • Multiprotocol routing:IP, IPX, AppleTalk, DLSw • Compact size, high availability and optimal cooling	1-35
Cisco 7400 Series Router	Highest performance 1 rack unit router inthe industry, with a stackable architecture that is designed for service provider and enterprise networks • One port adapter slot, two built-in 10/100/GE Ethernet ports, and a broad range of WAN media interfacesfrom DS0 to OC3 (40+ port adapters) common with Cisco 7x00-series port adapters • High-density broadband aggregation • Managed CPE for service provider demarcation point • Gigabit Ethernet to Gigabit Ethemet IP services applicationsplatform	1-38
Cisco 7500 Series	High-end services-enabled coreand WAN aggregation routerfor enterprise and service provider applications • 5-, 7-, and 13-slot models • 1-, 2-, or 4-bus models offering 1, 2, or 4 Gbps backplanes • Wide variety of LAN and WAN optionsincluding Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, serial, ISDN, HSSI, ATM, and Packet over SONET	1-40
Cisco 7600 Series	Service providerand high-end enterprise-class router delivering opticalWAN and Metropolitan Area Networkservices with high-touch IPservices at the networkedge. • Consolidated LAN/WAN/MAN in a single platform • Scalable backplane bandwidth from 32 Gbps to 256 Gbps and performance from 15 Mpps to 30 Mpps • High-volume aggregation of Ethernet traffic (server farms) • Wide range of WAN/MAN interfacesfrom NxDS0, T1, T3 to OC-48 with line rate services • Ideal for Internet data center, metropolitan aggregation, WAN edge aggregation, and enterprise core applications • Also supports Catalyst 6000 series line cards	1-45
Cisco 10000 Series	Service provider-class edge services router • High-Performance IP, MPLS, and Broadband Services — The Cisco 10000 Series enables service providers to deploy revenue-generating services without worrying about performance degradation • Carrier-Class High Availability — With its carrier-class high availability, the Cisco 10000 Series minimizes costly network outages and maximizing end-customer satisfaction • Application Integration — The Cisco 10000 Series leverages service providers' current investments by enabling leased line and broadband aggregationfeatures on a single platform • Application Flexibility — The Cisco 10000 Series has a broad range of channelized, clear channel, ATM and LAN interfaces. Physical interface speeds from E1/T1 up to OC-48c/STM-16c	1-47

Product	Features	Page
Cisco 10700 Series	Service provider-class metro edge services router • Optimized building blockfor the next generation metro Ethernet/IPaccess networks • Equipped with either (24) 10/100 or 4 GbE and 8 FE ports for customer access and OC-48c/STM-16c dynamic packet transport/resilient packet ring (DPT/RPR) technology or Packet Over SONET (POS) for metro optical connectivity • Powered by Cisco IOS 12.0S software and the parallel express forwarding (PXF) architecture • Cost-effective, reliable, high-performance platform supporting full suite of IP/MPLS features and services found in Cisco Internet Routers • With DPT/RPR architecture, enables optimal fiber connectivity as well as features such as IP class of service, VoIP, L2 VPN (EoMPLS and L2TPv3) and L3 VPN (MPLS) services	1-49
Cisco 12000 Series	Premier high-end routing portfolio for service provider backbone and high-speed edge applications. With its unique, modular distributed system architecture, the Cisco 12000 Series Router, is the industry choice for building Carrier IP/MPLS networks with its portfolio of 10Gbps systems and interfaces: • Seven chassis options that fit your scaling and real estate requirements offering the only complete solution for small to large POPs; backbone or edge. • The only platforms supporting backbone—or edge-optimized line cards in the same chassis, maximize the value of line-rate edge applications with 10G uplinks, and sustained line-rate performance as they scale to maximum capacity. • Proven investment protection with simple, field upgrades to higher switching capacities. • The only complete priority packet delivery solution set—the industry's only IP QoS implementation that uniquely enables premium real time IP services such as VoIP and video. • Extensive portfolio of line cards offering leading edge technologies (POS, ATM, DPT/RPR, GbE/FE), support a wide range of networking speeds (from DS1 to OC-192c/STM-64c). • The industry's only high-end router proven (via independent lab testing) to maintain customer connections and network traffic with zero packet loss despite a route processor failure.	1-51
Cisco SN 5400 Series Storage Router	Enables direct access to storage systems anywhere on an IP network. Enables SCSI over IP (iSCSI); the first storage implementation based on IP standards. • Cisco SN 5428: Migrates DAS (Direct Attached Storage) environments to SAN (Storage Area Networks) for small / medium businesses and enterprise workgroups. This is a full function Fibre Channel switch that adds iSCSI, providing very low price per port networked storage configurations	1-55

Sample Routing Solutions Overview—WAN & Internet Data Center



Cisco Routers Port Matrix

	SOHO Series	800 Series	1700 Series	2600 Series	3600 Series	3700 Series	7100 Series	7200 Series	7300 Series	7400 Series	7500 Series	7600 Series	10000 Series	10720 Series	12000 Series
Fixed Ports Only	X	X													
Fixed & Modular Ports			X	X	X[1]	X	X		X			X			
Modular Ports Only					X[2]			X		X	X		X	X	X
LAN Ports															
10-MB Ethernet	X	X	X	X	X	X	X	X		X	X	X		X	
10-MB Ethernet (fiber)					X		X	X		X	X	X			
100-MB Ethernet			X	X	X	X	X	X		X	X	X		X	X
100-MB Ethernet (fiber)					X		X	X		X	X	X	X	X	X
10/100-MB Eth	X	X	X	X	X	X	X	X						X	
Token Ring				X	X	X	X				X				
FDDI/CDDI											X				
ATM	X	X		X	X	X		X		X	X	X	X		
Gigabit Ethernet						X	X	X	X	X	X	X	X	X	X
WAN Ports															
Sync Serial		X	X	X	X	X		X		X	X	X			
Sync Serial w/ CSU			X	X	X	X							X		
ISDN BRI (S/T)		X	X	X	X	X	X	X		X	X				
ISDN BRI (U)		X	X	X	X	X	X	X		X	X				
ISDN PRI/Ch T1				X	X	X	X	X		X	X	X			
ISDN PRI w/ CSU				X	X	X		X		X	X	X			
Async			X	X	X	X									
Analog/POTS		X		X	X	X									
Integrated Modems				X	X	X									
Integrated Modem WICs			X	X	X	X									
HSSI				X[3]	X	X	X	X		X	X	X			
DS3				X	X	X	X	X		X	X	X	X		X
ATM OC-3				X[3]	X	X	X	X		X	X	X	X		X
ATM OC-12								X		X	X	X	X		X
ATM				X	X	X		X		X	X	X	X		X
ATM - T1/E1				X	X	X	X	X		X	X	X			
POS OC-x/STM-x							X	X	X	X	X	X	X		X
DPT/RPR OC-12/STM-4								X			X				X
DPT/RPR OC-48/STM-16												X	X	X	X
DPT/RPR OC-192/STM-64															X
ADSL	X	X	X	X	X	X									
ADSL over ISDN	X	X													
G.SHDSL	X	X	X	X		X									
IDSL		X	X	X		X									
DPT								X			X		X	X	X

	SOHO Series	800 Series	1700 Series	2600 Series	3600 Series	3700 Series	7100 Series	7200 Series	7300 Series	7400 Series	7500 Series	7600 Series	10000 Series	10720 Series	12000 Series
Voice Ports															
Analog		X	X	X	X	X									
Digital			X	X	X	X		X		X	X	X			
Integrated Switching															
Integrated 16-port Switching				X	X	X									
Integrated 36-port Switching					X[1]	X									
Inline Power				X[4]	X[4]	X									
Content Acceleration and Delivery															
Content Engine				X	X	X									
Security/VPN															
Encryption Advanced Integration Modules				X	X[1]	X									
Encryption Network Module					X[2]	X									

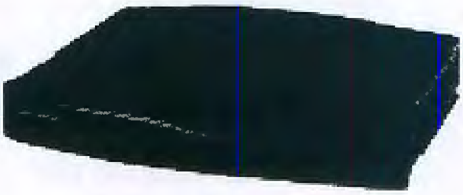
1. Cisco 3660 only
2. Cisco 3620 and 3640
3. Supported on the 2691 only
4. Requires external power source

Memory Information for Routers

Router	Memory Type	Slots	Default Memory	Max Memory	Default Configuration (Notes)
SOHO 78	Flash	1	8 MB	8 MB	No Upgradeable Memory
	DRAM	1	16 MB	16 MB	
SOHO 90	Flash	1	8 MB	8 MB	No Upgradeable Memory
	DRAM	1	32 MB	32 MB	
801, 802, 803, and 804	Flash	1	8 MB	12 MB	4MB on board and4MB or 8MB Mini flash card
	DRAM	1	4 MB	12 MB	4MB onboard and 4MB or 8MB DIMM module
805	Flash	1	4 MB	12 MB	
	DRAM	1	8 MB (On board)	16 MB	4MB On board + 4MB Mini Flash
811 and 813	Flash	1	8MB	12MB	4MB On board + 4MB or 8MB Mini Flash
	DRAM	1	8MB	16MB	8MB on board and4MB or 8MB DIMM Module
827-4V, 828	Flash	1	8 MB	16 MB	8MB On board + 4MB Mini Flash
	DRAM	1	16 MB (827-4V: 24 MB, 806: 32MB)	32 MB	16MB Onboard and 4MB or 8MB or 16MB DIMM Module
831, 836, 837	Flash	1	8 MB	24 MB	
	DRAM	1	32 MB	48 MB	
1721	Flash	1	16 MB	16 MB	Uses Mini Flash
	DRAM	1	32 MB (On board)	48 MB	
1751	Flash	1	16 MB	48 MB	
	DRAM	1	32 MB	96 MB	
1760	Flash	1	16 MB	64 MB	
	DRAM	1	32 MB	96 MB	
2500 Series	Flash	2	8 MB	16 MB	Slot 0 = 8 MB
	DRAM	1	4 MB	16 MB	
2600 Series	Flash (261xXM, 262xXM, 265xXM)	1	16 MB	48 MB	16 MB on Mother Board; Slot 0 = 32 MB
	Flash (261x)	1	8 MB	16 MB	Slot 0 = 8 MB
	Flash (262x,265x)	1	8 MB	32 MB	Slot 0 = 8 MB
	Flash (2691)	2	32 MB	128 MB	Slot 0 = 32 MB
	DRAM (261XM, 262xXM)	2	32 MB	128 MB	Slot 0 = 32 MB; Slot 1 = empty
	DRAM (265xXM)	2	64 MB	128 MB	Slot 0 = 64 MB; Slot 1 = empty
	DRAM (261x, 262x)	2	32 MB	64 MB	Slot 0 = 32 MB; Slot 1 = empty
	DRAM (265x)	2	32 MB	128 MB	Slot 0 = 32 MB; Slot 1 = empty
	DRAM (2691)	2	64 MB	256 MB	Slot 0 = 64 MB; Slot 1 = empty
3620 and 3640	Flash (PCMCIA)	2	0	32 MB	
	Flash (SIMM)	2	16 MB	32 MB	Slot 0 = 8 MB
	DRAM	4	32 MB	64 MB (3620) 128 MB (3640)	Slot 0 = 16 MB; Slot 1 = 16 MB
3660	Flash (PCMCIA)	2	0	32 MB	
	Flash (SIMM)	2	16 MB	64 MB	
	SDRAM	2	32 MB	256 MB	
3700	Flash (Internal)	1	32 MB	128 MB	
	Flash (External)	1	0 MB	32-128 MB	
	DRAM (SoDIMM)	2	128 MB	256 MB	Slot 0 = 128 MB
7100 Series	Flash (PCMCIA)	2	48 MB	110 MB	Slot 0 = 48 MB
	System SDRAM	2	64 MB	256 MB	Slot 0 = 64 MB
	Packet SDRAM		64 MB	64 MB	
7200 Series	Flash (PCMCIA)	2	20 MB	128 MB	
	Flash (non-volatile, fixed config)		128 KB	128 KB	
	Flash (C7200-IO-FE bootflash)	1	4 MB	4 MB	
	Flash (C7200-IO-2FE, C7200-IO-GE/E bootflash)	1	4 or 8 MB	4 or 8 MB	
	DRAM (NPE-225)	1	128 MB	256 MB	Slot 0 = 128 MB DIMM
	DRAM (NPE-300)	4	32+128 MB	32+256 MB	Slot 0 = 32 MB DIMM, Slot 2 = 128 MB DIMM
	DRAM (NPE-400)	1	128 MB	512 MB	Slot 0 = 128 MB SoDIMMs
	DRAM (NSE-1)	1	128 MB	256 MB	Slot 0 = 128 MB DIMM
	DRAM (NPE-G1)	1	256 MB	1 GB	Slot 0 = 128 MB SoDIMM, Slot 2 = 128 MB SoDIMM
7300 Series	Flash (CFM)	1	64 MB	128 MB	
	DRAM	1	128 MB	512 MB	

Router	Memory Type	Slots	Default Memory	Max Memory	Default Configuration (Notes)
7400 Series	Flash (PCMCIA)	2	64 MB	128 MB	
	DRAM (NSE-1) BB	1	256 MB	512 MB	
	DRAM (NSE-1) CP	1	128 MB	512 MB	
7500 Series	Flash (PCMCIA) RSP2, RSP4+	1	16 MB	20 MB	
	Flash (PCMCIA) RSP8	2	20 MB	40 MB	
	Flash (PCMCIA) RSP16	1	48 MB	128 MB	
	Flash (SIMM)	1	8 MB	8 MB	
	DRAM (RSP2)	4	32 MB	128 MB	
	DRAM (RSP4+, RSP8)	2	64 MB	256 MB	
	DRAM (RSP16)	2	128 MB	1 GB	
	DRAM (VIP2-40)	1	32 MB	64 MB	
	DRAM (VIP2-50)	1	32 MB	128 MB	
	DRAM (VIP4-50/80)	1	64 MB	256 MB	
	DRAM (VIP6-80)	1	64 MB	256 MB	
7600 Series	Flash (PCMCIA)	1	16MB	20 MB	
	DRAM (Sup 2)	1	128MB	512 MB	
	DRAM (MSFC2)	1	128MB	512 MB	
	DRAM (PFC2)	1	128MB	256 MB	
10000 Series	Flash (PCMCIA)	2	48 MB	128 MB	1 x 48MB ships as default; 128MB is optional
	Flash (Internal)	1	32 MB	32 MB	
	Shared (PRE-1)	1	128 MB	128 MB	
	DRAM (PRE-1)	1	512 MB	512 MB	
10700 Series	Flash (Internal)	1	32 MB	64 MB	Maximum memory is configured with No Option
	SDRAM RP	1	256 MB	256 MB	
	Packet Buffer	1	64 MB	64 MB	
12000 Series	Flash (PCMCIA)	2	20 MB	20 MB	
	DRAM (GRP-B)	1/2	128 MB	512 MB	Route Memory
	SDRAM (PRP-1)	1/2	512 MB	1 GB	Route Memory
	DRAM (Line Cards)	1/2	128-256 MB	256-512 MB	Route Memory (line card dependent)
	SDRAM (Line Cards)	1/2	128-256 MB	256-512 MB	Packet Memory (line card dependent)
	Shared (PRE-2)	1	128 MB	128 MB	
	DRAM (PRE-2)	1	512 MB	512 MB	

Cisco SOHO Series Ethernet, ADSL over ISDN, ADSL and G.SHDSL Routers



The Cisco SOHOseries provides an affordable, secure, multi-user access solution to small office/home office (SOHO) customers while reducing deployment and operational costs for service providers. Through the power of Cisco IOS software technology, the Cisco SOHO 91 Ethernet to Ethernet Router, the SOHO 96 ADSL over ISDN, the SOHO 97 ADSL and SOHO 78 G.SHDSL routers provide superior manageability and reliability.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco SOHO 91	• Ethernet WAN port for use with an external DSL or cable modem with 4-port 10/100 switch, stateful firewall and software based encryption
Cisco SOHO 96	• ADSL modem for use of ADSL over ISDN with 4-port 10/100 switch, stateful firewall and software based encryption
Cisco SOHO 97	• ADSL modem for ADSL over POTS with 4-port 10/100 switch, stateful firewall and software based encryption
Cisco SOHO 78	• 4-port Ethernet Hub and 1G.SHDSL port with firewall security and Cisco IOS manageabilty and reliability

Key Features

- Integrated security of Cisco IOS Software with Stateful Inspection Firewall and software-based 3DES encryption (no encryption on the SOHO 78)
- Easy setup and deployment using Cisco Router Web Set Up Tool (CRWS)
- Offers many local and remote debug and troubleshooting features in Cisco IOS Software

Competitive Products

- 3Com: OfficeConnect 810
- Alcatel: Speed Touch Pro Router
- Cayman: 3220H
- Efficient: 5861, 5660
- Lucent: CellPipe 50A
- Netopia: R6100, 4533
- Westel: Wirespeed 36R566
- Zyxel: 641, 782
- Nokia: MW1352
- Linksys: Etherfast models

Specifications

Feature	SOHO 91	SOHO 96	SOHO 97	SOHO 78
Fixed LAN Ports	4-port 10/100 Switch	4-port 10/100 Switch	4-port 10/100 Switch	4-port Ethernet (10BASE-T)
Fixed WAN Ports	1-port Ethernet (connects to external DSL or cable modem	1-port ADSL over ISDN	1-port ADSL over POTS	1-port G.SHDSL
Flash Memory	8 MB	8 MB	8 MB	8 MB
DRAM Memory	32 MB	32 MB	32 MB	16 MB
Dimensions (HxWxD)	2.0 x 9.7 x 8.5 in.	2.0 x 9.7 x 8.5 in.	2.0 x 9.7 x 8.5 in.	2.0 x 9.9 x 8.3 in. (5.1 x 25.2 x 21.1 cm)

For More Information

See the Cisco SOHO Web site: **http://www.cisco.com/go/soho90**

Cisco 800 Series

The Cisco 800 series router provides enhanced network security and proven reliability through Cisco IOS software, for small offices and telecommuters. It connects users to the Internet or to a corporate LAN via one ADSL, ADSL over ISDN, G.SHDSL, IDSL, ISDN, or serial connection (up to 512 Kbps), or with an Ethernet WAN port connected to an external broadband modem.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 800 Series	• Companies who Cisco IOS-based networks who want to add telecommuters • Service providers who offer value-added services to small offices • VARs who are familiar with Cisco IOS software and want to profitably service small office customers • Ethernet LAN ports and variety of WAN connectivity, including: ISDN BRI, Frame Relay, ADSL, G.SHDSL, async dialup (see Specificationsfor details)

Key Features

- Fixed configuration support for several types of WAN connections
- Standard security with ACLs, PAT/NAT, PAP/CHAP, MS-CHAP, Lock and Key, and Generic Routing Encapsulation (GRE) tunneling
- Enhanced security with stateful inspection firewall, IPSec encryption (hardware based on Cisco 830s and AES encryption on Cisco 830s)
- Toll quality voice with VoIP on Cisco 827-4V
- Integrated 4-port 10/100 Ethernet Switch on Cisco 830 series
- Bandwidth optimization features such as compression, Bandwidth-on-Demand, Dial-on-Demand, Always-On-Dynamic-ISDN (AODI), and X.25 over D channel (Cisco 801- 804)
- Support for CAPI applications in the European market

Competitive Products

- 3Com: Office Connect Remote 511/521
- Alcatel: Speed Touch Pro Routers
- Ascend: Pipeline 75/85
- Efficient: 5861 / 5660
- Intel: Express 8100
- Netopia: R3100, R6100, 4533
- Nortel/Bay: Nautica 250
- Nokia: MW1352
- Zyxel: 782
- Linksys: Etherfast

Specifications

Cisco 801, 802, 803, 804, 805, 811 and 813

Feature	801	802	803	804	811	813
Fixed LAN Port Connections	1-port Ethernet (10BASE-T)	1-port Ethernet (10BASE-T)	4-port Ethernet hub (10BASE-T)	4-port Ethernet hub (10BASE-T)	1-port Ethernet (10BASE-T)	4-port Ethernet hub (10BASE-T)
Fixed WAN Port Connections	1-port ISDN BRI (S/T)	1-port ISDN BRI (U) NT-1	1-port ISDN BRI (S/T) 2 analog ports	1-port ISDN BRI (U) NT-1 2 analog ports	1-port ISDN BRI S/T and 1-port ISDN BRI (U) NT-1	1-port ISDN BRI S/T and 1-port ISDN BRI (U) NT-1 2 analog ports
Flash Memory	8MB (default) 12 MB (max)	8MB (default) 12 MB (max)	8MB (default) 12 MB (max)	8MB (default) 12 MB (max)	4MB (default) 12MB (max)	8MB (default) 12MB (max)
DRAM Memory	4MB (default) 12MB (max)	4MB (default) 12MB (max)	4MB (default) 12MB (max)	4MB (default) 12MB (max)	8MB (default) 16MB (max)	8MB (default) 16MB (max)
Dimensions (HxWxD)	2.0 x 9.9 x 8.3 in. (5.1 x 25.2 x 21.1 cm)	Same as Cisco 801	Same as Cisco 801	Same as Cisco 801	Same as Cisco 801	Same as Cisco 801

Cisco 800 Series (805, 836, 827-4V, 828, 836, 837)

Feature	805	827-4V	828	831	836	837
Fixed LAN Port Connections	1-port Ethernet (10BASE-T)	1-port Ethernet (10BASE-T)	4-port Ethernet hub (10BASE-T)	4-port Ethernet (10BASE-T)	1-port Ethernet (10BASE-T)	4-port Ethernet (10BASE-T)
Fixed WAN Port Connections	1-port Serial (Up to 512 KBPS)	1-port ADSL	1-port G.SHDSL	1-port Ethernet	1-port ADSL-over-ISDN, 1-port ISDN S/T	1-port ADSL over POTS
Flash Memory	4MB (default) 12MB (max)	8MB (default) 16MB (max)	8MB (default) 16MB (max)	8MB (default) 24MB (max)	8MB (default) 24MB (max)	8MB (default) 24MB (max)
DRAM Memory	8MB (default) 16MB (max)	24MB (default) 32MB (max)	16MB (default) 32MB (max)	32MB (default) 48MB (max)	32MB (default) 48MB (max)	32MB (default) 48MB (max)
Dimensions (HxWxD)	2.0 x 9.9 x 8.3 in. (5.1 x 25.2 x 21.1 cm)	Same as Cisco 805	Same as Cisco 805	2.0 x 9.7 x 8.5 in.	2.0 x 9.7 x 8.5 in.	2.0 x 9.7 x 8.5 in.

Selected Part Numbers and Ordering Information[1]

Cisco 800 Series Routers	
CISCO801	1-port 10BASE-T, 1-port BRI (S/T), IP s/w
CISCO802	1-port 10BASE-T, 1-port BRI (U) w/ NT-1, IP s/w
CISCO803	4-port 10BASE-T hub, 1-port BRI (S/T), 2-port POTS, IP s/w
CISCO804	4-port 10BASE-T hub, 1-port BRI (U) w/ NT-1, 2-port POTS, IP s/w
CISCO805	1-port 10BASE-T, 1-port serial, IP s/w
CISCO801-CAPI	ISDN/Ethernet Router with one-user CAPI license
CISCO803-CAPI	ISDN/Ethernet Router with one-user CAPI license, 4-port hub
CISCO827-4V	1-port ADSL, 1-port 10BASE-T, 4 ports FXS, IP/Voice s/w
CISCO828	1-port G.SHDSL, 4-port 10BASE-T hub, IP s/w
CISCO831-K9 USD 649.00	Cisco 831 Ethernet Router
CISCO836-K9	Cisco 836 ADSL over ISDN Router
CISCO837-K9	Cisco 837 ADSL Router
Cisco 800 Series CD Feature Packs	
CD08-BHL-12.0.7XV=	Cisco 800 Series IP/IPX/FW Plus IPSec 56
CD08-BP-12.07.XV=	Cisco 800 Series IP/IPX/Plus
CD800-5CAPI=	CAPI 5 User CD
CD08-IC-12.0.5T=	Cisco 800 Series Internet DSL
CD08-ICHL-12.0.5T=	Cisco 800 Series Internet DSL FW IPSec56
CD08-IBHL-12.0.5T=	Cisco 800 Series Internet DSL IPX FW IPSec56
Cisco 800 Series Memory Options	
MEM800-4F=	Cisco 800 Series, 4 MB Flash Mini-Card
MEM800-8F=	Cisco 800 Series, 8 MB Flash Mini-Card
MEM800-4D=	Cisco 800 Series, 4 MB DRAM DIMM
MEM800-8D=	Cisco 800 Series, 8 MB DRAM DIMM
MEM820-8U16F	Cisco 820 Flash upgrade 8Mbyte-16Mbyte
MEM820-16U20D	Cisco 820 DRAM upgrade 16Mbyte-20Mbyte (16Mbyte-24Mbyte & 16Mbyte-32Mbyte also available)
MEM820-24U32D	Cisco 820 DRAM 24Mbyte upgrade to 32 Mbytes
Cisco 800 Series Accessories	
PWR-8xx-WW1=	Cisco 8xx Series, AC Power Supply Spare
Cisco 800 Series Basic Maintenance	
CON-SNT-PKG1	Cisco 800 Series SMARTnet Maintenance (8x5xNBD)

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco 800 Series Web site: **http://www.cisco.com/go/800**

Cisco 1700 Series

The Cisco 1700 series modular access routers are designed to provide a cost-effective integrated access platform for small and medium-sized businesses and enterprise small branch offices. These Cisco IOS-based routers deliver high-speed network access, comprehensive security features, and multiservice data/voice/video/fax integration to meet the most demanding business requirements. Within the Cisco 1700 series, Cisco 1710 security access routers work with existing broadband modems to provide advanced routing and security functionality, Cisco 1721 modular access routers provide flexible, high-performance data access, and Cisco 1751 and Cisco 1760 modular access routers are optimized for both voice and data traffic, providing a simple and cost-effective path to multi-service networking—today or in the future.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 1710	• Advanced routing and security functionalityin one device when connecting to the Internet using a broadband modem • Hardware-assisted 3DES VPN encryption at fullT1/E1 speeds
Cisco 1721	• Secure data-only access solution that adapts to customers' evolving network requirements • Support for data applicationsincluding VPNs and broadband access services • A broad array of WAN services supported, including Frame Relay, leased line, ADSL, G.SHDSL, ISDN BRI, X.25, SMDS and more • IPSec 3DES VPN encryption at full T1/E1 speeds • IEEE 802.1Q VLAN Support
Cisco 1751	All the above, plus: • Analog and digital voice support in a desk-top form factor • 3 modular slots for WAN and Voice interface cards
Cisco 1760	All the above, plus: • 19" rackmount form factor • 4 slots with 2 WIC/VIC and 2 VIC slots • Multiservice analog anddigital voice support • Highest performance multi-service router in the Cisco 1700 family • Higher density analog and digital voice support than Cisco 1751

Key Features

- Support for up to 4 serial interfaces or 2 ISDN BRI; 1 autosensing 10/100 Mbps Fast Ethernet LAN connection; 1 auxiliary (AUX) port for dial-up management or low-speed asynchronous connections (up to 112.5 kbps)
- Flexibility—Cisco 1700 Series supports a diverse set of WAN and Voice Interface Cards that are shared with the 1600 (WAN only), 2600/2600XM, and 3600 series routers enabling field upgradeability to evolve with the needs of growing businesses
- Integrated Device—Cisco 1700 series combines WAN routing, VPN and multiservice access in a single device
- Expansion Slot—Supports optional hardware VPN module for wire-speed IPSec 3DES encryption and can enable future technologies (VPN Module standard on Cisco 1710)
- Integrated Security—The 1700 series supports context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, Java blocking, real-time alerts, Intrusion Detection System (IDS), and encryption.
- IEEE 802.1Q VLAN Support

Specifications

Feature	Cisco 1710	Cisco 1721	Cisco 1751/1751-V	Cisco 1760/1760-V
Fixed LAN Ports (connections)	1-port autosensing 10/100 Mbps Ethernet	1-port autosensing 10/100 Mbps Ethernet	1-port autosensing 10/100 Mbps Ethernet	1-port autosensing10/100 Mbps Ethernet
Fixed WAN Ports	1-port 10BASE-T Ethernet for broadband modem	None	None	None
Modular Slots	None	2 WAN slots	3 slots (2 WAN or Voice slots and 1 Voice-only slot)	4 Slots (2 WAN or Voice slots and 2 Voice-only slots)
WAN Interface Card (WIC) Modules	None	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Voice Interface Cards (VIC) Modules	None	None	See Part Numbersand Ordering Information	See Part Numbers and Ordering Information
Flash Memory	16 MB Flash (default/max)	16 MB (default); 16 MB (max)	1751 base model: 16 MB (default); 16MB (max) 1751-V multiservice ready configuration: 32 MB (default); 32 MB (max)	1760 base model: 16-MB Flash Memory (on board) 64-MB (max) 1760-V: 32-MB Flash 64-MB (max)
DRAM Memory	64 MB	32 MB (default);96 MB (max)	1751 base model: 32 MB (default); 96MB (max) 1751-V multiservice-ready configuration:64 MB (default); 96MB (max)	1760 base model:32 MB (default)96 MB (max)1760-V:64 MB (default)96 MB (max)
Dimensions (HxWxD)	3.1 x 11.2 x 8.7 in.	3.1 x 11.2 x 8.7 in.	4.0 x 11.2 x 8.7 in.	1.7 x 17.5 x 12.8 in.

Cisco IOS Software and Memory Requirements[1]

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required	DRAM Memory Required
C017-C- 12.x	IP only IP/ADSL	12.1 Mainline	4 MB 8 MB	16 MB 20 MB
CD17-CH-12.x	IP/FW	12.1 Mainline	4 MB	20 MB
CD17-CP-12.x	IP Plus	12.1 Mainline	4 MB	20 MB
CD17-CHK2-12.x	IP/FW Plus IPSEC 3DES	12.1 Mainline	8 MB	32 MB
CD17-CVP-12.x	IP/Voice Plus	12.1 Mainline	8 MB	24 MB
CD17-CHV-12.x	IP/FW/Voice Plus	12.1 Mainline	8 MB	24 MB
CD17-CHVK2-12.x	IP/FW/Voice Plus IPSEC 3DES	12.1 Mainline	8 MB	24 MB
CD17-C- 12.x	IP only	12.1T	4 MB	16 MB
CD17-CH-12.x	IP/FW	12.1T	4 MB	20 MB
CD17-CP-12.x	IP Plus	12.1T	8 MB	24 MB
CD17-CK2-12.x	IP Plus IPSEC 3DES	12.1T	8 MB	32 MB
CD17-CHK2-12.x	IP/FW Plus IPSEC 3DES	12.1T	8 MB	32 MB
CD17-CVP-12.x	IP/Voice Plus	12.1T	8 MB	32 MB
CD17-CHV-12.x	IP/FW/Voice Plus	12.1T	8 MB	32 MB
CD17-CVK2-12.x	IP/Voice Plus IPSEC 3DES	12.1T	8 MB	32 MB
CD17-CHVK2-12.x	IP/FW/Voice Plus IPSEC 3DES	12.1T	8 MB	32 MB

[1] For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information." For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

Selected Part Numbers and Ordering Information[1]

Cisco 1700 Series Modular Access Routers

CISCO1760	10/100 Modular Router w/ 2WIC/VIC,2VIC slots,19 inch Chassis
CISCO1760-ADSL	10/100 BaseT Modular Router w/ADSL WIC, IP/ADSL
CISCO1760-SHDSL	10/100 BaseT Modular G.SHDSL Router, 19 inch Chassis
CISCO1760-VPN/K9	1760 VPN Bundle with VPN Module, 48MB DRAM, IP Plus/FW/3DES
CISCO1760-VPN/K9-A	1760 VPN Bun. w/ADSL WIC, VPN Module, 48MB DRAM, IP+/FW/3DES
CISCO1760-V	10/100 Modular Router w/Voice IP/VOICE Plus, 19 inch Chassis
CISCO1751	10/100 Modular Router w/ 3 slots, IOS IP, 16F/32D
CISCO1751-V	10/100 Modular Router w/Voice, IOS IP/VOICE Plus, 32F/64D
CISCO1751-VPN/K9	1751 VPN Bundle with VPN Module, 48MB DRAM, IP Plus/FW/3DES
CISCO1751-VPN/K9-A	1751 VPN Bun. w/ADSL WIC, VPN Module, 48MB DRAM, IP+/FW/3DES
CISCO1721-ADSL	10/100 BaseT Modular ADSL Router, IP/DSL

CISCO1721	10/100BaseT Modular Router w/2 WAN slots, 16M Flash/32M DRAM
CISCO1721-VPN/K9	1721 VPN Bundle with VPN Module, 48MB DRAM, IP Plus/FW/3DES
CISCD1721-VPN/K9-A	1721 VPN Bun. w/ADSL WIC, VPN Module, 48MB DRAM, IP+/FW/3DES
CISCO1721-SHDSL	10/100 BaseT Modular G.SHDSL Router, IP/DSL
CISCO1710-VPN-M/K9	Dual-Ethernet SecurityAccess Router, VPN Module, IP/3DES/FW

Cisco 1751 Software Feature Packs for Cisco IOS Release 12.1.(5)YB

CD17-C-12.1.5=	IP
CD17-C-12.1.5=	IP ADSL
CD17-C7P-12.1.5=	IP Plus ADSL
CD17-C7K2-12.1.5=	IP Plus IPSec 3DES ADSL
CD17-CH-12.1.5=	IP/FW/IDS
CD17-B-12.1.5=	IP/IPX
CD17-B7HP-12.1.5=	IP/IPX/FW/IDS Plus ADSL
CD17-C7HK2-12.1.5=	IP/FW/IDS Plus IPSec 3DES ADSL
CD17-Q7HK2-12.1.5=	IP/IPX/AT/IBM/FW/IDS Plus IPSec 3DES
CD17-C7VP-12.1.5=	IP/Voice Plus
CD17-C7VP-12.1.5=	IP/Voice Plus ADSL
CD17-C7HV-12.1.5=	IP/Voice/FW/IDS Plus ADSL
CD17-C7VK2-12.1.5=	IP/Voice Plus IPSec 3DES ADSL
CD17-C7HVK2-12.1.5=	IP/Voice/FW/IDS Plus IPSec 3DES ADSL
CD17-Q7HVK2-12.1.5=	IP/IPX/AT/IBM/FW/IDS/Voice Plus IPSec 3DES

Cisco 1700 Series Memory Options

MEM-1700-4MFC=	Cisco 1700 Series, 4 MB Mini-Flash Card
MEM-1700-8MFC=	Cisco 1700 Series, 8 MB Mini-Flash Card
MEM-1700-16D=	Cisco 1700 Series, 16 MB DRAM DIMM
MEM-1700-32D=	Cisco 1700 Series, 32 MB DRAM DIMM
MEM-1700-64D+	Cisco 1700 Series, 64 MB DRAM DIMM

Cisco 1700 Series WAN Interface Cards (WICs)

WIC-1T	1-port Serial WAN Interface Card
WIC-2T	2-port Serial WAN Interface Card
WIC-2A/S	2-port Async/Sync Serial WAN Interface Card
WIC-1B-S/T	1-port BRI (S/T) WAN Interface Card (dialand leased line)
WIC-1B-U	1-port BRI w/NT-1 WAN Interface Card (dialand leased line)
WIC-1DSU-56K4	1-port 4-Wire 56/64 Kbps w/ (DSU/CSU) WAN Interface Card
WIC-1DSU-T1	1-port T1/Fr T1 w/ (DSU/CSU) WAN Interface Card
WIC-1ADSL=	1-port ADSL WAN Interface Card
WIC-1SHDSL	1-port G.SHDSL WAN Interface Card
WIC-1ENET=	1-port Ethernet Interface Card

Cisco 1751/1760 Voice Interface Cards

VIC-2FXS	2-port Voice Interface Card FXS
VIC-4FXS	4-port Voice Interface Card FXS
VIC-2FXO	2-port Voice Interface Card FXO
VIC-2E/M	2-port Voice Interface Card E&M
VIC-2FXO-EU	2-port Voice Interface Card FXO for Europe
VIC-2FXO-M	32-port Voice Interface Card FXO for Australia
VIC-2BRI-NT/TE	2-port Voice Interface Card—BR (NT & TE)
VIC-2FXO-M1	2-port FXO for U.S. with batteryreversal
VIC-2FXO-M2	2-port FXO for Europe with batteryreversal
VIC-2DID	2-port FXO analog DID

Cisco 1700 Multiflex Voice / WAN interface Cards

VWIC-1MFT-E1	1-Port RJ-48 Multiflex Trunk - E1
VWIC-1MFT-E1=	1-Port RJ-48 Multiflex Trunk - E1
VWIC-1MFT-G703	1-Port RJ-48 Multiflex Trunk - G.703
VWIC-1MFT-G703=	1-Port RJ-48 Multiflex Trunk - G.703
VWIC-2MFT-E1	2-Port RJ-48 Multiflex Trunk - E1
VWIC-2MFT-E1=	2-Port RJ-48 Multiflex Trunk - E1
VWIC-2MFT-E1-DI	2-Port RJ-48 Multiflex Trunk - E1 With Drop and Insert
VWIC-2MFT-E1-DI=	2-Port RJ-48 Multiflex Trunk - E1 With Drop and Insert
VWIC-2MFT-G703	2-Port RJ-48 Multiflex Trunk - G.703
VWIC-2MFT-G703=	2-Port RJ-48 Multiflex Trunk - G.703
VWIC-1MFT-T1	1-Port RJ-48 Multiflex Trunk - T1
VWIC-1MFT-T1=	1-Port RJ-48 Multiflex Trunk - T1
VWIC-2MFT-T1-DI	2-Port RJ-48 Multiflex Trunk - T1 With Drop and Insert
VWIC-2MFT-T1-DI=	2-Port RJ-48 Multiflex Trunk - T1 With Drop and Insert
VWIC-2MFT-T1	2-Port RJ-48 Multiflex Trunk - T1
VWIC-2MFT-T1=	2-Port RJ-48 Multiflex Trunk - T1

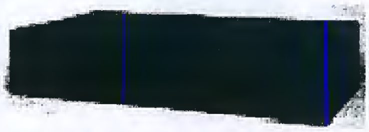
Cisco 1700 Module Options	
MOD1700-VPN	Cisco 1700 Series VPN Module
Cisco 1700 Spares and Accessories	
PWR-1700-WW1=	Cisco 1700 AC Power Supply—worldwide
PVDM-256K-4=	4-Channel Packet Voice/Fax DSP Module for the 1751
PVDM-256K-8=	8-Channel Packet Voice/Fax DSP Module for the 1751
PVDM-256K-12=	12-Channel Packet Voice/Fax DSP Module for the 1751
PVDM-256K-16=	16-Channel Packet Voice/Fax DSP Module for the 1751
PVDM-256K-20=	20-Channel Packet Voice/Fax DSP Module for the 1751
Cisco 1700 Series Basic Maintenance	
CON-SNT-PKG4	Cisco 1751-V SMARTnet Maintenance
CON-SNT-PKG3	Cisco 1751 and 1710-VPN-M/K9 SMARTnet Maintenance
CON-SNT-PKG2	Cisco 1720 and 1720-ADSL SMARTnet Maintenance

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco 1700 Series Web site: **http://www.cisco.com/go/1700**

Cisco 2500 Series



The Cisco 2500 series router has served for years as the most deployed and popular branch office router in the world, and provides low cost routing functionality for data-only applications (no voice support). There are currently two access servers to choose from, 8 or 16 asynchronous ports, each with 1 Ethernet port, for aggregating multiple network elements to provide a single Telnet access point (telemetry application)—or for attaching 8 to 16 external analog or digital modems in environments where T1/E1 digital circuits are not available, but multiple dial-up telephone lines can be leveraged for low cost remote access.

For higher performance requirements, where a wider variety of WAN/LAN interfaces are needed, as well as voice support, refer to Cisco 2600/2600XM/3600 or 1700 series routers.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco AS2509-RJ and AS2511-RJ	• Data-only network requirement • An access server combining a terminal server, protocol translator, console port aggregator, and a router in a single device • One Ethernet LAN and dual serial ports • 8 or 16 asynchronous serial ports with RJ-11 jacks, ideal for attaching 8 to 16 external modems

Key Features

- Proven technology with a full suite of Cisco IOS Software
- Setup with Cisco ConfigMaker, a free tool for configuring a network of routers
- With CiscoWorks for Windows, allows remote management and maintenance from a central location

Specifications

Feature	Cisco AS2509-RJ	Cisco AS2511-RJ
Throughput Performance (pps)	3-5 Kpps (dependingon configuration)	3-5 Kpps (depending on configuration)
Memory	8-MB dual Flash bank option (default) 16 MB (max) 16 MB DRAM (default)	Same as Cisco AS2509-RJ
Power Supply	AC, with optional DC or redundant power supply	Same as Cisco AS2509-RJ
Fixed LAN Ports	1-port Ethernet	1-port Ethernet
Fixed WAN Ports	1-port sync serial 8-port async	1-port sync serial 16-port async
Dimensions (H x W x D)	1.75 x 17.5 x 10.56 in.	1.75 x 17.5 x 10.56 in.

Cisco IOS Software and Memory Requirements

To run the Cisco IOS software Feature Packs, you need the amount of memory shown in the following table:

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required[2]	DRAM Memory Required
CD25-C-12.0=	IP only	12.0(10) 12.0(7)T	8 MB 8 MB	4 MB 6 MB
CD25-CP-12.0=	IP Plus	12.0(10) 12.0(7)T	8 MB 16 MB	6 MB 8 MB
CD25-CHL-12.0=	IP/FW Plus IPSEC 56	12.0(10) 12.0(7)T	16 MB 16 MB	8 MB 10 MB
CD25-B-12.0=	IP/IPX/AT/DEC	12.0(10) 12.0(7)T	8 MB **16 MB**	6 MB 6 MB
CD25-BP-12.0=	IP/IPX/AT/DEC Plus	12.0(10) 12.0(7)T	16 MB 16 MB	6 MB 8 MB
CD25-AP-12.0=	Enterprise Plus	12.0(10) 12.0(7)T	16 MB 16 MB	6 MB 10 MB

[1] For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

[2] Bold numbers indicate that more memory than the default amount is needed to run the Feature Pack.

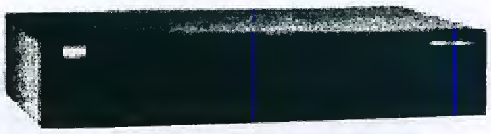
Selected Part Numbers and Ordering Information[1]

Cisco 2500 Series Access Router Chassis	
CISCO2509-CH	1-port Ethernet AUI, 2-port Serial, 8-port Async Serial, IP s/q
AS2509-RJ-CH	1-port Ethernet AUI (RJ-45), 1-port Serial, 8-port Async Serial, IP s/w
CISCO2511-CH	1-port Ethernet AUI, 2-port Serial, 16-port Async Serial, IP s/w
AS2511-RJ-CH	1-port Ethernet AUI (RJ-45), 1-port Serial, 16-port Async Serial, IP s/w
Cisco 2500 Series Memory Options	
MEM-1X4F=	Cisco 2500 Series, 4 MB Flash Upgrade
MEM-1X8F=	Cisco 2500 Series, 8 MB Flash Upgrade
MEM-1X8D=	Cisco 2500 Series, 8 MB DRAM Upgrade
MEM-1X16D=	Cisco 2500 Series, 16 MB DRAM Upgrade
Cisco 2500 Series Accessories	
ACS-2500RM-19=	Cisco 2500 Series, Rack-Mount Kit, 19 Inches
ACS-2500RM-24=	Cisco 2500 Series, Rack-Mount Kit, 24 Inches
ACS-2500ASYN=	Cisco 2500 AUX/Console Part Cable Kit
ACS-2500RPS=	Cisco 2500 Series, RPS Field Upgrade
Cisco 2500 Series Basic Maintenance	
CON-SNT-PKG4	Packaged SMARTnet (8 x5 x NBD) for the Cisco AS2509 and AS2511

For More Information

See the Cisco 2500 Series Web site: **http://www.cisco.com/go/2500**

Cisco 2600 Series



The Cisco 2600 series is an award-winning family of modular multiservice access routers, providing flexible LAN and WAN configurations, multiple security options, voice/data integration, and a range of high performance processors. This range of features make the Cisco 2600 series the ideal branch-office router for today's and tomorrow's customer requirements.

The Cisco 2600 series family of modular routers include the Cisco 2600XM models, the Cisco 2691 and the Cisco 2612 token ring router. These new models deliver extended performance, higher density, enhanced security performance and increased concurrent application support to meet the growing demands of branch offices.

The Cisco 2600XM models are based on the classic Cisco 2600 platform architecture, and extend the performance by as much as 33%. They also increase default platform memory and provide increases in memory capacity at the same price as their Cisco 2600 predecessor.

The highest performing router in the Cisco 2600 family that extends the density of emerging branch office applications, is the Cisco 2691 offering almost twice the performance of the Cisco 2650XM platform while leveraging the same modules from other Cisco 2600, Cisco 3600 and Cisco 3700 Series routers. Compared to the Cisco 2600XM models, the new Cisco 2691 is designed to offer a higher degree of versatility, providing greater throughput for higher density WAN applications, support for high speed interfaces and increased performance to handle new services.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 2691	• Enterprises wanting a higherlevel of performance for a broadened range of concurrent remote office applications including unparalleled voice/data integraton, Virtual Private Network (VPN) performance, increased bandwidth to suppot voice and video applications and the delivery of Web-based applications
Cisco 2600XM Series	• Enterprises consideringthe Cisco 2600 for branch office applicationsshould now regard the Cisco 2600XM as the preferential platformfor delivering high performing, flexible solutions to branch and remote offices
	• High Performance 10/100 Dual Ethernet Router with 3 WIC Slots, 1 NM
Cisco 2651XM	• High performance Dual10/100 Modular Router with CiscoIOS IP
Cisco 2650XM	• High performance 10/100 Modular Router with Cisco IOS IP
Cisco 2621XM	• Mid Performance Dual10/100 EthernetRouter with Cisco IOS IP
Cisco 2620XM	• Mid Performance 10/100 Ethemet Router with Cisco IOS IP
Cisco 2611XM	• Dual 10/100 Ethemet Router with Cisco IOS IP
Cisco 2610XM	• 10/100 Ethernet Router with Cisco IOS IP
Cisco 2612	• One Token Ring port and one Ethernet port formixed LANs and migrating from Token Ring to Ethemet

Key Features

- Integration/manageability—Lowers cost of ownership and improves ease of remote management, providing integrated "branch-in-a-box" networking that combines CSU/DSUs, multiplexors, modems, voice/data gateways, ISDN NT1s, firewalls, VPNs, encryption, and compression devices
- Multiservice voice/data networks—Reduces phone/fax costs between offices; using Cisco IOS software QoS features (such as RSVP, WFQ, CAR, and RED), voice/fax traffic is digitized and encapsulated in Frame Relay or IP packets and consolidated with data traffic

- Enterprise/Provider class solution—Meets the requirements of multiservice enterprises and their managed service CPE providers with high reliability features, multiple WAN connections, and the ability to migrate from data- only to TDM voice and data to packetized voice and data infrastructure
- High-density analog/fax network modules provide the ability to directly connect PSTN and legacy telephony equipment to existing Cisco 2600 and 3600 routers
- An EtherSwitch network module for the Cisco 2600/3600 series with 16 ports of 10/100 Ethernet and one optional 1000BaseT (Gigabit Ethernet) connection, providing a fully integrated Layer 2 (L2) switch with the capability to support both Line Power to Cisco IP phones and current Aironet 802.11 wireless base stations (with the addition of an external power supply). This provides a single box solution for branch offices deploying converged IP telephony, extending data, voice and video by delivering IP routing, Ethernet switching, fixed wireless solutions and voice gateway capabilities
- A wide range of Virtual Private Network modules (VPN) optimize the Cisco 2600 Series platforms for virtual private networks (VPNs) and delivers a rich integrated package of routing, firewall, intrusion-detection, and VPN functions
- The introduction of the WIC-ADSL and WIC-1SHDSL, offers business-class broadband service with scalable performance, flexibility, and security for branch and regional offices
- Content Networking Integration and Branch-Office Routing with router-integrated content-delivery system that combines intelligent caching, content routing and management with robust branch-office routing, WAN bandwidth for branch IP services such as voice over IP (VoIP)

Competitive Products

- 3Com: SuperStack II NETBuilder SI and PathbuilderS400
- Intel/Shiva: LanRover Family
- Motorola: Vanguard 645x/643x
- Nortel/Bay: Advanced Remote Node (ARN), Passport 4400 series
- FutureWei/Quidway®: R2630/31E
- Tasman: 2004, 1400

Specifications

Feature	2610/11XM	2620/21XM	2650/51XM	2691
Performance	Up to 20Kpps	Up to 30Kpps	Up to 40Kpps	Up to 70Kpps
Flash Memory (Default/Max)	16MB/48MB	16MB/48MB	16MB/48MB	32MB/128MB (Compact Flash)
System Memory (Default/Max)	32MB/128MB	32MB/128MB	64MB/128MB	64MB/256MB
Integrated WIC Slots	2	2	2	3
Onboard AIM Slot	1	1	1	2
Minimum Cisco IOS Release	12.1(14) mainline, 12.2(12) mainline, 12.2(8)T1or later	12.1(14) mainline, 12.2(12) mainline, 12.2(8)T1or later	12.1(14) mainline, 12.2(12) mainline, 12.2(8)T1or later	12.2(8)T1 or later
Onboard LAN Ports	1 to 2 10/100 FE ports	1 to 2 10/100 FE ports	1 to 2 10/100 FE ports	2 10/100 FE ports
Rack Mounting	Yes, 19" and 23" options	Yes, 19" and 23" options	Yes, 19" and 23" options	Yes, 19" and 23" options
Wall Mounting	Yes	Yes	Yes	No

Cisco IOS Software and Memory Requirements[1]

Most Cisco IOS software CD feature packs for the Cisco 2600 series include several selected Cisco IOS releases. To run the latest Cisco IOS Software Feature Packs with version 12.0(7)XK, you need, at a minimum, the amount of memory shown in the following table. Some configurations will require more than the recommended minimum.

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required	DRAM Memory Required
Cisco 2612				
CD26-C-12.0.7=	IP only	12.0(7)XK1	8 MB	24 MB
CD26-CP-12.0.7=	IP Plus	12.0(7)XK1	8 MB	40 MB
CD26-CH-12.0.7=	IP/Firewall	12.0(7)XK1	8 MB	32 MB
CD26-CHL-12.0.7=	IP/Firewall Plus IPSec 56	12.0(7)XK1	16 MB	48 MB
CD26-CHK2-12.0.7=	IP/Firewall Plus IPSec 3DES	12.0(7)XK1	16 MB	48 MB
CD26-CK2-12.0.7=	IP Plus IPSec 3DES	12.0(7)XK1	16 MB	40 MB
CD26-CL-12.0.7=	IP Plus IPSec 56	12.0(7)XK1	16 MB	40 MB
CD26-B-12.0.7=	IP/IPX/AT/DEC	12.0(7)XK1	8 MB	32 MB
CD26-BP-12.0.7=	IP/IPX/AT/DEC Plus	12.0(7)XK1	16 MB	40 MB
CD26-BHP-12.0.7=	IP/IPX/AT/DEC/Firewall Plus	12.0(7)XK1	16 MB	48 MB
CD26-AP-12.0.7=	Enterprise Plus	12.0(7)XK1	16 MB	48 MB
CD26-AL-12.0.7=	Enterprise Plus IPSec 56	12.0(7)XK1	16 MB	48 MB
CD26-AHK2-12.0.7=	Enterprise/Firewall Plus IPSec 3DES	12.0(7)XK1	16 MB	48 MB
CD26-AHL-12.0.7=	Enterprise/Firewall Plus IPSec 56	12.0(7)XK1	16 MB	48 MB
CD26-AK2-12.0.7=	Enterprise Plus IPSec 3DES	12.0(7)XK1	16 MB	48 MB
CD26-E-12.0.7=	Remote Access Server	12.0(7)XK1	8 MB	24 MB

[1] For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information." For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

Selected Part Numbers and Ordering Information[1]

Cisco 2600/2600XM Series Router Chassis	
CISCD2610XM	10/100 Ethernet Router w/Cisco IOS IP
CISCO2610XM-DC	10/100 Ethernet Router w/ Cisco IOS IP - DC
CISCO2610XM-RPS	10/100 Ethemet Router w/ Cisco IOS IP - use w/ ext RPS
CISCO2611XM	Dual 10/100 Ethernet Router w/ Cisco IOS IP
CISCO2611XM-DC	Dual 10/100 Ethernet Router w/ CiscoIOS IP - DC
CISCO2611XM-RPS	Dual 10/100 Ethernet Router w/ Cisco IOS IP - use w/ ext RPS
CISCO2620XM	Mid Performance 10/100 Ethernet Router with Cisco IOS IP
CISCO2620XM-DC	Mid Performance10/100 Ethemet Router w/Cisco IOS IP-DC
CISCO2620XM-RPS	Mid Performance 10/100 Ethernet Rout w/Cisco IOS IP-RPS ADPT
CISCO2621XM	Mid Performance Dual 10/100 Ethernet Router w/Cisco IOS IP
CISCO2621XM-DC	Mid Performance Dual10/100 Ethernet Rout w/Cisco IOS IP-DC
CISCO2621XM-RPS	Mid Performance Dual 10/100 Ethemet Rout w/IOS IP-RPS ADPT
CISCO2650XM	High Performance 10/100 Modular Router w/Cisco IOS IP
CISCO2650XM-DC	High Performance 10/100 Modular Rout w/CiscoIOS IP-DC NEBs
CISCO2650XM-RPS	High Performance 10/100 Modular Rout w/CiscoIOS IP-RPS ADPT
CISCO2651XM	High Performance Dual 10/100 Modular Rout with CiscoIOS IP
CISCO2651XM-DC	High Performance Dual 10/100 Modular Rout w/IP-DC NEB
CISCO2651XM-RPS	High Performance Dual 10/100 Mod Rout w/IP-RPS ADPT
CISCO2691	High Performance 10/100 Dual Eth Router w/3 WIC Slots,1 NM
CISCO2612	1-port 10BASE-T, 1-port TR, 1 network module slot, 1 AIM slot, 2 WIC slots, IP s/w
CISCO2612-DC	1-port 10BASE-T, 1-port TR, 1 network module slot, 1 AIM slot, 2 WIC slots, DC Power Supply, IP s/w
CISCO2612-RPS	1-port 10BASE-T, 1-port TR, 1 network module slot, 1 AIM slot, 2 WIC slots, RPS adapter, IP s/w
Cisco 2600 Series Voice Gateway Bundles	
CISCO2651XM-V	CISCO2651XM, AIM-VOICE-30, IOS IP Plus, 96D/32F
CISCO2651XM-V-SRST	CISCO2651XM, FL-SRST-MEDIUM, AIM-VOICE-30, IOS IP Plus, 96D/32F

Cisco 2600 Series VPN Bundles

CVPN2600FIPS/KIT=	KIT (Instructions, labels) to configued 2600 for FIPS
C2651XM-2FE/VPN/K9	2651XM/VPN Bundle, AIM-VPN/EP/2FE/IOS FW/IPSec 3 DES, 96DRAM
C2621XM-2FE/VPN/K9	2621XM/VPN Bundle, AIM-VPN/EP/2FE/IOS FW/IPSec 3 DES, 96DRAM
C2611XM-2FE/VPN/K9	2611XM/VPN Bundle, AIM-VPN/EP/2FE/IOS FW/IPSec 3 DES, 96DRAM
C2691-VPN/K9	2691 VPN Bundle,AIM-VPN/EPII, Plus IOS/FW/IPSEC3DES

Cisco 2600 Series DSL Bundles

CISCO2651XM-ADSL	2651XM-ADSL Bundle, WIC-1ADSL, 2FE, IP Plus, 32F/96DRAM
CISCO2621XM-ADSL	2621XM-ADSL Bundle, WIC-1ADSL, 2FE, IP Plus, 32F/96DRAM
CISCO2611XM-ADSL	2611XM-ADSL Bundle, WIC-1ADSL, 2FE, IP Plus, 32F/96DRAM
CISCO2651XM-SHDSL	2651XM-SHDSL Bundle, WIC-1SHDSL, 2FE, IP Plus, 32F/96DRAM
CISCO2621XM-SHDSL	2621XM-SHDSL Bundle, WIC-1SHDSL, 2FE, IP Plus, 32F/96DRAM
CISCO2611XM-SHDSL	2611XM-SHDSL Bundle, WIC-1SHDSL, 2FE, IP Plus, 32F/96DRAM

Cisco 2600/2600XM Series LAN Modules

NM-1E=	1-port 10BASE-T network module
NM-4E=	4-port 10BASE-T network module

Cisco 2600/2600XM and 3600 Series WAN Interface Cards (WICs)

WIC-1B-S/T=	1-port BRI (S/T) WAN Interface Card (Dialand Leased Line)
WIC-1B-U-V2	1-port BRI (U) w/NT-1 WAN Interface Card (Dialand Leased Line)
WIC-1DSU-56K4=	1-port Serial W/ 4-Wire 56/64Kbps DSU/CSU WAN Interface Card
WIC-1DSU-T1=	1-port Serial w/ FrT1/T1 DSU/CSU WAN Interface Card
WIC-1T=	1-port Serial WAN Interface Card
WIC-2T=	2-port Serial WAN Interface Card
WIC-2A/S=	2-port Async/Sync Serial WAN Interface Card
WIC-1ADSL=	1-port ADSL WAN Interface Card
WIC-1SHDSL=	1-port G.SHDSL WAN Interface Card
WIC-1AM=	1-port Analog Modem WAN Interface Card
WIC-2AM=	2-port Analog Modem WAN Interface Card

Cisco 2600/2600XM and 3600 Series Multiflex Voice and WAN Interface Cards[2]

VWIC-1MFT-T1=	1-port RJ-48 Multiflex TrunkT1
VWIC-2MFT-T1=	2-port RJ-48 Multiflex Trunk—T1
VWIC-2MFT-T1-DI=	2-port RJ-48 Multiflex Trunk—T1 With Drop and Insert
VWIC-1MFT-E1=	1-port RJ-48 Multiflex Trunk—E1
VWIC-1MFT-G703=	1-port RJ-48 Multiflex Trunk-G.703
VWIC-2MFT-E1=	2-port RJ-48 Multiflex Trunk—E1
VWIC-2MFT-G703=	2-port RJ-48 Multiflex Trunk-G.703
VWIC-2MFT-E1-DI=	2-port RJ-48 Multiflex Trunk—E1 With Drop and Insert

Cisco 2600/2600XM and 3600 Series Voice/Fax Network Modules and Expansion Modules

NM-1V=	1-slot voice/fax network module
NM-2V=	2-slot voice/fax network module
NM-HDV-1T1-24=	1-port T1 24 channel voice/fax network module
NM-HDV-1T1-24E=	1-port T1 24 enhanced channelvoice/faxnetwork module
NM-HDV-2T1-48=	2-port T1 48 channel voice/fax network module
NM-CE-BP-20G-K9=	Content Engine NM-Basic Perf-20GB
NM-CE-BP-40G-K9=	Content Engine NM-Basic Perf-40GB
NM-CE-BP-SCSI-K9=	Content Engine NM-Basic Perf-SCSI Adapter
NM-HDV-1E1-30=	1-port E1 30 channel voice/fax network module
NM-HDV-1E1-30E=	1-port E1 30 enhanced channelvoice/faxnetwork module
NM-HDV-2E1-60=	2-port E1 60 channel voice/fax network module
NM-HDV=	High density voice network module, spare (no T1/E1 or DSPs)
NM-HDA-4FXS=	High density analog voice/fax network module with 4 FXS
EM-HDA-8FXS=	8-port FXS voice/fax expansion module
EM-HDA-4FXO=	4-port FXO voice/fax expansion module
DSP-HDA-16	16-channel DSP module for NM-HDA

Cisco 2600/2600XM and 3600 Series ATM Modules

NM-4T1-IMA=	4-port T1 ATM network module with IMA
NM-4E1-IMA=	4-port E1 ATM network module with IMA
NM-8T1-IMA=	8-port T1 ATM network module with IMA
NM-8E1-IMA=	8-port E1 ATM network module with IMA

Cisco 2600/2600XM and 3600 Series EtherSwitch Modules

NM-16ESW=	Sixteen 10BaseT/100BaseTX autosensing ports EtherSwitch
NM-16ESW-PWR=	Sixteen 10BaseT/100BaseTX autosensing ports EtherSwitch with power daughter card

Cisco 2600/2600XM and 3600 Series High-Density Voice/Fax DSP Upgrade Modules

PVDM-12=	12-channel Packet Voice/Fax DSP Module

Cisco 2600/2600XM and 3600 Series Voice Interface Cards (VICs)

VIC-2E/M=	2-port E&M Voice Interface Card
VIC-2FXO=	2-port FXO Voice Interface Card
VIC-2FXS=	2-port FXS Voice Interface Card
VIC-2DID=	2-port DID Voice/Fax Interface Card
VIC-2FXO-EU=	2-port FXO Voice InterfaceCard (for Europe)
VIC-2FXO-M3=	2-port FXO Voice Interface Card (forAustralia)
VIC-2BRI-S/T-TE=	2-port BRI (S/T user side) Voice Interface Card
VIC-2FXO-M1=	2-port Voice Interface Card—FXO w/ Reversal (for US+)
VIC-2FXO-M2=	2-port Voice Interface Card—FXO w/ Reversal (for EU)

Cisco 2600/2600XM and 3600 Series WAN Network Modules

NM-4B-S/T=	4-port BRI (S/T) networkmodule
NM-8B-S/T=	8-port BRI (S/T) networkmodule
NM-4B-U=	4-port BRI (U) w/ NT1 network module
NM-8B-U=	8-port BRI (U) w/ NT1 network module
NM-4A/S=	4-port Async/Sync Serial network module
NM-8A/S=	8-port Async/Sync Serial network module
NM-16A=	16-port Async Serial network module
NM-32A=	32-port Async Serial network module
NM-1CT1=	1-port Channelized T1/ISDN-PRI network module
NM-2CT1=	2-port Channelized T1/ISDN-PRI network module
NM-1CT1-CSU=	1-port Channelized T1/ISDN-PRI w/ CSU network module
NM-2CT1-CSU=	2-port Channelized T1/ISDN-PRI w/ CSU network module
NM-1ATM-25=	1-port ATM 25 network module

Cisco 2600/2600XM and 3600 Series Modem Network Modules

NM-8AM=	8-port Analog Modem network module
NM-16AM=	16-port Analog Modem networkmodule

Cisco 2600/2600XM and 3600 Series Network Modules (International)

NM-1CE1B=	1-port Channelized E1/ISDN-PRI balanced networkmodule
NM-1CE1U=	1-port Channelized E1/ISDN-PRI unbalanced networkmodule
NM-2CE1B=	2-port Channelized E1/ISDN-PRI balanced networkmodule
NM-2CE1U=	2-port Channelized E1/ISDN-PRI unbalanced networkmodule

Cisco 2600/2600XM and 3600 Series Modem Management Technology Licenses (MMTL)[3]

MMTL-3600/2600-8=	MMTL for 8 Analog Modems
MMTL-3600/2600-16=	MMTL for 16 Analog Modems

Cisco 2600/2600XM Series Advanced Integration Modules

AIM-COMPR2=	Data Compression AIM for the Cisco 2600/2600XM series
AIM-COMPR4=	Data Compression AIM for the Cisco 2691/3660/3700 series
AIM-VPN/BP=	DES/3DES VPN Encryption AIMfor 2600-Base Performance
AIM-ATM=	ATM SAR Only AIM
AIM-ATM-1T1=	High Performance ATM AIM/T1 Bundle AIM-ATM
AIM-ATM-1E1=	High Performance ATM AIM/E1 Bundle AIM-ATM
AIM-VPN/-EP=	DES/3DES VPN Encryption Module for 2600-Enhanced Performance
AIM-VPN/-EPII=	DES/3DES/AES VPN Encryption Module for 2691/3725
AIM-ATM-VOICE-30=	30-Channel T1/E1 Digital Voice Module
AIM-VOICE-30=	SAR and 30-Channel T1/E1 Digital Voice Module

Cisco 260/2600XM0 Series Factory Memory Options

Product Number	Product Description
MEM2691-32CF-EXT	32MB External Compact Flash Memory for the 2691
MEM2691-64CF-EXT	64MB External Cisco Flash Memory for the 2691
MEM2691-128CF-EXT	128MB External Cisco Flash Memory for 2691

Cisco 2600/2600XM Series Factory DRAM Memory Upgrades

MEM2600-32U40D	32- to 40-MB DRAM Factory Upgrade for the Cisco 2600 Series
MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade for the Cisco 2600 Series
MEM2600-32U64D	32- to 64-MB DRAM Factory Upgrade for the Cisco 2600 Series
MEM2650-32U40D	32 TO 40MB DRAM Factory Upgrade for the Cisco 265x only
MEM2650-32U48D	32 TO 48MB DRAM Factory Upgrade for the Cisco 265x only
MEM2650-32U64D	32 TO 64MB DRAM Factory Upgrade for the Cisco 265x only
MEM2650-32U96D	32 TO 96MB DRAM Factory Upgrade for the Cisco 265x only
MEM2650-32U128D	32 TO 128MB DRAM Factory Upgrade for the Cisco 265x only
MEM2600XM-32U128D	32 to 128MB DRAM factory upgrade for Cisco 261x/2xXM
MEM2600XM-32U64D	32 to 64MB DRAM factory upgrade for Cisco 261x/2xXM
MEM2600XM-32U96D	32 to 96MB DRAM factory upgrade for Cisco 261x/2xXM
MEM2600XM-64U128D	64 to 128MB DRAM factory upgrade - 265xXM/XM VPN Bundles
MEM2600XM-64U96D	64 to 96MB DRAM factory upgrade - 265xXM/XM VPN Bundles
MEM2691-64U128D	64 to 128MB DIMM DRAM factory upgrade for the Cisco 2691
MEM2691-64U192D	64 to 192MB DIMM DRAM factory upgrade for the Cisco 2691

MEM2691-64U256D	64 to 256MB DIMM DRAM factory upgrade for the Cisco 2691
Cisco 2600/2600XM Series Factory Flash Memory Upgrades	
MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series
MEM2620-8U32FS	8 TO 32MB Flash SIMM Upgrade for the Cisco262x only
MEM2650-8U32FS	8 TO 32MB Flash SIMM Upgrade for the Cisco265x only
MEM2600XM-16U32FS	16 to 32 MB Flash Factory Upgrade for the Cisco 2600XM
MEM2600XM-16U48FS	16 to 48MB Flash Factory Upgrade for the Cisco 2600XM
MEM2691-32U128CF	32 to 128MB Cisco 2691 Compact Flash factory upgrade
MEM2691-32U64CF	32 to 64MB Cisco 2691 Compact Flash factory
MEM-CE-256U512D	256MB DRAM Factory Upgrade for NM-CE-BP
Cisco 2600/2600XM Series Memory Spares	
MEM2600-8D=	8 MB DRAM DIMM for the Cisco 2600 Series
MEM2600-16D=	16 MB DRAM DIMM for the Cisco 2600 Series
MEM2600-32D=	32 MB DRAM DIMM for the Cisco 2600 Series
MEM2600-4FS=	4 MB Flash SIMM for the Cisco 2600 Series
MEM2600-8FS=	8 MB Flash SIMM for the Cisco 2600 Series
MEM2600-16FS=	16 MB Flash SIMM for the Cisco 2600 Series
MEM2620-32FSBOOT=	32MB FLASH SIMM and BOOTROM for 262x Only
MEM2650-32FS=	32MB Flash SIMM for the Cisco 265x only
MEM2650-8D=	8MB DRAM DIMM for the Cisco 265x only
MEM2650-16D=	16MB DRAM DIMM for the Cisco 265x only
MEM2650-32D=	32MB DRAM DIMM for the Cisco 265x only
MEM2650-64D=	64MB DRAM DIMM for the Cisco 265x only
MEM2600XM-16FS=	16MB Flash SIMM for the Cisco 2600XM
MEM2600XM-32D=	32MB DIMM DRAM for the Cisco 2600XM
MEM2600XM-32FS=	32MB Flash SIMM for the Cisco 2600XM
MEM2600XM-64D=	64MB DIMM DRAM for the Cisco 2600XM
MEM2691-128CF=	128MB Cisco 2691 Compact Flash Memory
MEM2691-128D=	128MB DIMM DRAM for the Cisco 2691
MEM2691-32CF=	32MB Cisco 2691 Compact Flash Memory
MEM2691-64CF=	64MB Cisco 2691 Compact Flash Memory
MEM2691-64D=	64MB DIMM DRAM for the Cisco 2691
MEM-CE-256D=	256MB DRAM Field Upgrade for NM-CE-BP
Cisco 2600/2600XM Series Spares - Power Supplies and Other	
PWR-2600-AC=	Cisco 2600/2600XM AC power supply spare
PWR-2600-DC=	Cisco 2600/2600XM DC power supply spare
PWR-2650-AC=	Cisco265x AC power supply spare
ACS-2600RPS=	RPS Field Upgrade for the Cisco 2600 Series
ACS-2600RM-19=	19 Inch Rack Mount Kit for the Cisco2600 series
ACS-2600RM-24=	24 Inch/23 Inch Rack Mount Kit for the Cisco 2600 Series
ACS-2600ASYN=	Auxiliary and Console Port Cable Kit for Cisco 2600 Series
ACS-2600NEBS/ETSI=	NEBS/ETSI Telco Accessory Kit for Cisco 2600
CAB-RPS-2218	RPS 22/18 Load Cable
CAB-RPS-2218=	RPS 22/18 Load Cable
CAB-RPSY-2218	RPS 22/18 Two-to-one DC Power Cable
CAB-RPSY-2218=	RPS 22/18 Two-to-one DC Power Cable
PWR600-AC-RPS-CAB	600W Redundant AC Power System With DC Power Cables
PWR600-AC-RPS-NCAB	600W Redundant AC Power System W/O DC Power Cables
BOOT-2600=	Boot ROM for Cisco 2600 Series
Cisco 2600/2600XM Series SMARTnet Maintenance	
CON-SNT-PKG5	Cisco 2600 Series Packaged SMARTnet 8x5xNBD Maintenance
Cisco 2691 Series Network Modules	
NM-1GE=	1 Port GE Network Module
NM-1T3/E3=	One port T3/E3 network module

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).
2. VoIP and VoFR require use of a Voice/Fax network module
3. Requires Plus feature pack

For More Information

See the Cisco 2600 Series Web site: **http://www.cisco.com/go/2600**

Cisco 3600 Series

The Cisco 3600 Series is a family of modular, high-performance multiservice access routers for medium and large-sized branch offices and Internet service providers. With over 100 modular interface options (shares modular interfaces with the 2600/2600XM series), the Cisco 3600 Series provides solutions for voice/data integration, virtual private networks (VPNs), dial access, and multiprotocol data routing. Using Cisco's digital and analog voice/fax network modules, the Cisco 3600 Series allows customers to consolidate voice, fax, and data traffic on a single network. Its architecture protects customers' investment in network technology and integrates the functions of several devices into a single, manageable solution. Cisco 3600 VPN and Dial Bundles are also available to also address specific VPN/security, and dial-up remote access server requirements. Customers are encouraged to migrate to the Cisco 3700 Series.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 3620	• Medium-density WAN and dialup connectivity • Medium-density LAN connectivity • Low-density Voice over Data • Low-density ATM connections • Mid-density modem-over-PRI bundles
Cisco 3640A	• High-density WAN and dialup connectivity • Medium- to high-density LAN connectivity • Mid-density Voice over Data • Low- to mid-density ATM connections • Low-density modem-over-BRI bundles • Configurationsnot available on the Cisco 3700
Cisco 3660	• Very high-density WAN and dialup connectivty • High-density LAN connectivity • Mid-density Voice over Data • Mid-density ATM connections • Mid- to high-density modem-over-PRI and BRI connectivity

Key Features

- Combines dial access, advanced LAN-to-LAN routing services, ATM connectivity, and multiservice integration of voice, video, and data in a single platform
- Modular, scalable design provides performance, scalability, flexibility, and investment protection
- High-density ISDN PRI capabilities
- Preconfigured BRI and PRI modem bundles available
- Support for modem-over-BRI functionality
- Integrated Cisco IOS software (base price includes IP IOS software)
- Full VPN and Firewall support
- ADSL and G.SHDSL support
- ISDN Modem backup

Specifications

Feature	Cisco 3620	Cisco 3640	Cisco 3660
Fixed Ports	None	None	1 or 2 10/100 Fast Ethernet
Network Module Slots	2	4	6
Advanced Integration Module (AIM) Slots	None	None	2
LAN/Combo Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
WAN Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620 (Hardware compression support only through AIM-COMPR4)
ATM Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Voice/Fax Network Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
WAN Interface Card (WIC) Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Multiflex Voice/WAN Interface Cards	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Voice Interface Card (VIC) Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Modem Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Performance	40 kpps	50-70 kpps	100-120 kpps
Flash Memory	8 MB (default);32 MB (max)	Same as Cisco 3620	8 MB (default); 64MB (max)
DRAM Memory	32 MB (default) 64 MB (max)	32 MB (default) 128 MB (max)	32 MB SDRAM (default) 256 MB SDRAM (max)
Power Supply	AC, DC optional	AC, DC optional	Single or dual AC/DC
Dimensions (HxWxD)	1.75 x 17.5 x 13.5 in.	3.44 x 17.5 x 15 in.	8.7 x 17.5 x 11.8 in.

Cisco IOS Software and Memory Requirements[1]

To run the Cisco IOS Feature Packs, you need the following amount of memory:

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required[2]	DRAM Memory Required
Cisco 3620 and 3640				
CD36-C-12.0.7=	IP only	12.0(7)XK	8 MB	32 MB
CD36-CP-12.0.7=	IP Plus	12.0(7)XK	16 MB	48 MB
CD36-CH-12.0.7=	IP/FW	12.0(7)XK	8 MB	32 MB
CD36-CHL-12.0.7=	IP/FW Plus IPSec 56	12.0(7)XK	16 MB	64 MB
CD36-CHK2-12.0.7=	IP/FW Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB
CD36-CK2-12.0.7=	IP/ Plus IPSec 3DES	12.0(7)XK	16 MB	48 MB
CD36-CL-12.0.7=	IP Plus IPSec 56	12.0(7)XK	16 MB	48 MB
CD36-B-12.0.7=	IP/IPX/AppleTalk/DECnet	12.0(7)XK	8 MB	32 MB
CD36-BP-12.0.7=	IP/IPX/AppleTalk/DECnet Plus	12.0(7)XK	16 MB	48 MB
CD36-BHP-12.0.7=	IP/IPX/AT/DEC/FW Plus	12.0(7)XK	16 MB	64 MB
CD36-AP-12.0.7=	Enterprise Plus	12.0(7)XK	16 MB	64 MB
CD36-AL-12.0.7=	Enterprise Plus IPSec 56	12.0(7)XK	16 MB	64 MB
CD36-AHK2-12.0.7=	Enterprise/FW Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB
CD36-AHL-12.0.7=	Enterprise/FW Plus IPSec 56	12.0(7)XK	16 MB	64 MB
Cisco 3660				
CD36-C-12.0.7=	IP only	12.0(7)XK	8 MB	32 MB SDRAM
CD36-CP-12.0.7=	IP Plus	12.0(7)XK	16 MB	64 MB SDRAM
CD36-CH-12.0.7=	IP/FW	12.0(7)XK	8 MB	64 MB SDRAM
CD36-CHL-12.0.7=	IP/FW Plus IPSec 56	12.0(7)XK	16 MB	64 MB SDRAM
CD36-CHK2-12.0.7=	IP/FW Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB SDRAM
CD36-CK2-12.0.7=	IP/ Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB SDRAM
CD36-CL-12.0.7=	IP Plus IPSec 56	12.0(7)XK	16 MB	64 MB SDRAM
CD36-B-12.0.7=	IP/IPX/AppleTalk/DECnet	12.0(7)XK	8 MB	64 MB SDRAM
CD36-BP-12.0.7=	IP/IPX/AppleTalk/DECnet Plus	12.0(7)XK	16 MB	64 MB SDRAM

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required[2]	DRAM Memory Required
CD36-BHP-12.0.7=	IP/IPX/AT/DEC/FW Plus	12.0(7)XK	16 MB	64 MB SDRAM
CD36-AP-12.0.7=	Enterprise Plus	12.0(7)XK	16 MB	64 MB SDRAM
CD36-AL-12.0.7=	Enterprise Plus IPSec 56	12.0(7)XK	16 MB	64 MB SDRAM
CD36-AHK2-12.0.7=	Enterprise/FW Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB SDRAM
CD36-AHL-12.0.7=	Enterprise/FW Plus IPSec 56	12.0(7)XK	16 MB	64 MB SDRAM

1. For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information". For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn
2. Bold numbers indicate that more memory than the default amount is needed to run the Feature Pack.

Selected Part Numbers and Ordering Information[1]

Cisco 3600 Series Router Chassis

CISCO3620	2-slot Modular Router-AC Power Supply, IP s/w
CISCO3620-DC	2-slot Modular Router-DC Power Supply, IP s/w
CISCO3620-RPS	2-slot Modular Router, w/ RPS, IP s/w
CISCO3640	4-slot Modular Router-AC Power Supply, IP s/w
CISCO3640-DC	4-slot Modular Router-DC Power Supply, IP s/w
CISCO3640-RPS	4-slot Modular Router, w/ RPS, IP s/w
CISCO3661-DC	10/100 E Cisco 3660 6-slot Modular Router-DC with IP SW
CISCO3661-AC	10/100 E Cisco 3660 6-slot Modular Router-AC with IP SW
CISCO3662-DC	Dual 10/100 E Cisco 3660 6-slot Modular Router-DC with IP SW
CISCO3662-AC	Dual 10/100 E Cisco 3660 6-slot Modular Router-AC with IP SW

Cisco 3600 Series Bundles

3640MBUNDLE-4B-S/T	3640 BRI Dial bundle. Includes 1E2W,12DM, 4 BRI-S/T, IP IOS
3640MBUNDLE-4B-U	3640 BRI Dial bundle. Includes 1E2W,12DM, 4 BRI-U, IP IOS
3640MBUNDLE-8B-S/T	3640 BRI Dial bundle. Includes 1E2W,18DM, 8 BRI-S/T, IP IOS
3640MBUNDLE-8B-U	3640 BRI Dial bundle. Includes 1E2W,18DM, 8 BRI-U, IP IOS
3620MBUNDLE-24DM	3620 PRI Dial bundle. Includes 1FE2CT1-CSU, 24DM, IP IOS
AS3640-T1-48DM	3600 Access Concentrator, 48 MICA Modems, 2 PRI/T1, Ethernet, IP IOS
AS3640-E1-60DM	3600 Access Concentrator, 60 MICA Modems, Ethernet, IP IOS, no PRI

Cisco 2600/2600XM and 3600 Series ATM Modules[2]

Cisco 2600/2600XM and 3600 Series WAN Interface Cards (WICs)[2]

Cisco 2600/2600XM and 3600 Series Multiflex Voice/WAN Interface Cards[2]

Cisco 2600/2600XM and 3600 Series Voice/Fax Network Modules[2]

Cisco 2600/2600XM and 3600 Series High-Density Voice/Fax DSP Upgrade Modules[2]

Cisco 2600/2600XM and 3600 Series Network Modules (International)[2]

Cisco 3600 Series LAN/Combo Network Modules

NM-1E=	1-port 10BASE-T Network Module
NM-4E=	4-port 10BASE-T Network Module
NM-1FE-TX=	1-port 100BASE-TX Network Module
NM-1FE-FX=	1-port 100BASE-FX Network Module
NM-1E2W=	1-port 10BASE-T, 2 WIC Slots Network Module
NM-2E2W=	2-port 10BASE-T, 2 WIC Slots Network Module
NM-1E1R2W=	1-port 10BASE-T, 1-port Token Ring, 2 WIC Slots Network Module
NM-1FE1CT1=	1-port 100BASE-TX, 1-port Channelized T1/ISDN-PRI Network Module
NM-1FE1CT1-CSU=	1-port 100BASE-TX, 1-port Channelized T1/ISDN-PRI with CSU Network Module
NM-1FE1CE1B=	1-port 100BASE-TX, 1-port Channelized E1/ISDN-PRI (Balanced) Network Module
NM-1FE1CE1U=	1-port 100BASE-TX, 1-port Channelized E1/ISDN-PRI (Unbalanced) Network Module
NM-1FE2CT1=	1-port 100BASE-TX, 2-port Channelized T1/ISDN-PRI Network Module
NM-1FE2CT1-CSU=	1-port 100BASE-TX, 2-port Channelized T1/ISDN-PRI with CSU Network Module
NM-1FE2CE1B=	1-port 100BASE-TX, 2-port Channelized E1/ISDN-PRI (Balanced) Network Module
NM-1FE2CE1U=	1-port 100BASE-TX, 2-port Channelized E1/ISDN-PRI (Unbalanced) Network Module
NM-1FE2W=	1-port 10/100 Ethernet, 2 WIC Slots Network Module
NM-2FE2W=	2-port 10/100 Ethernet, 2 WIC Slots Network Module
NM-1FE1R2W=	1-port 10/100 Ethernet, 1-port Token Ring, 2 WIC Slots Network Module
NM-2W=	2 WIC Slots Network Module

Cisco 3600 Series Voice Interface (VIC) Cards

VIC-2E/M=	2-port Voice Interface Card—E&M
VIC-2FXO=	2-port Voice Interface Card—FXO
VIC-2FXS=	2-port Voice Interface Card—FXS
VIC-2BRI-S/T-TE=	2-port Voice Interface Card—BRI (S/T user side)
VIC-2DID=	2-port Voice Interface Card—Direct Inward Dial (DID)
VIC-2FXO-EU=	2-port Voice Interface Card—FXO (for Europe)

Cisco 3600 Series WAN Modules

NM-4B-S/T=	4-port BRI (S/T) Module
NM-8B-S/T=	8-port BRI (S/T) Module
NM-4B-U=	4-port BRI (U) w/ NT-1 Module
NM-8B-U=	8-port BRI (U) w/ NT-1 Module
NM-4T=	4-port Serial Module
NM-4A/S=	4-port Async/Sync Serial Module
NM-8A/S=	8-port Async/Sync Serial Module
NM-16A=	16-port Async Module
NM-32A=	32-port Async Module
NM-1CT1=	1-port Channelized T1/ISDN-PRI Module
NM-1CT1-CSU=	1-port Channelized T1/ISDN-PRI w/ CSU Module
NM-2CT1=	2-port Channelized T1/ISDN-PRI Module
NM-2CT1-CSU=	2-port Channelized T1/ISDN-PRI w/ CSU Module
NM-1HSSI=	1-port HSSI Module
NM-COMPR=	Compression Module
NM-VPN/MP=	DES/3DES VPN Encryption NM for the 3620/3640 Mid-Platform

Cisco 3660 AIM Modules

AIM-VPN/HP=	DES/3DES VPN Encryption AIM for 3660 High Performance
AIM-COMPR4=	Data Compression AIM for the 3600 series
AIM-ATM=	ATM SAR Only ATM
AIM-ATM-VOICE-30=	30-Channel T1/E1 Digital Voice Module
AIM-VOICE-30=	SAR and 30-Channel T1/E1 Digital Voice Module

Cisco 3620/40 VPN Module

NM-VPN/MP=	DES/3DES VPN Encryption NM for 3620/3640 Mid Performance

Cisco 3600 Series Modem Modules

NM-6DM=	6-port Digital Modem Module
NM-8AM=	8-port Analog Modem Module
NM-12DM=	12-port Digital Modem Module
NM-16AM=	16-port Analog Modem Module
NM-18DM=	18-port Digital Modem Module
NM-24DM=	24-port Digital Modem Module
NM-30DM=	30-port Digital Modem Module
MICA-6MOD=	6-port Digital Modem Module (Spare)

Cisco 3600 Series Modem Management Technology Licenses[3]

MMTL-3600-6=	Modem Management Technology License (6 modems)
MMTL-3600-12=	Modem Management Technology License (12 modems)
MMTL-3600-18=	Modem Management Technology License (18 modems)
MMTL-3600-24=	Modem Management Technology License (24 modems)
MMTL-3600-30=	Modem Management Technology License (30 modems)
MMTL-3600/2600-8=	Modem Management Technology License (for 8 Analog Modems)
MMTL-3600/2600-16=	Modem Management Technology License (for 16 Analog Modems)

Cisco 3600 Series Memory Options

MEM3600-8FC=	Cisco 3600 Series 8 MB Flash PCMCIA Card
MEM3600-16FC=	Cisco 3600 Series 16MB Flash Card
MEM3600-8FS=	Cisco 3600 Series 8 MB Flash
MEM3600-16FS=	Cisco 3600 Series 16 MB Flash
MEM3600-2X8FS=	Cisco 3600, 16 MB Flash (2x8 MB Flash SIMMs)
MEM3600-2X16FS=	Cisco 3600, 32 MB Flash (2x16 MB Flash SIMMs)
MEM3620-8D=	Cisco 3620, 8 MB DRAM SIMM
MEM3620-16D=	Cisco 3620, 16 MB DRAM SIMM
MEM3640-2X8D=	Cisco 3640, 16 MB DRAM (2x8 MB DRAM SIMMs)
MEM3640-2X16D=	Cisco 3640, 32 MB DRAM (2x16 MB DRAM SIMMs)
MEM3640-2X32D=	Cisco 3640, 64 MB DRAM (2x32MB DRAM SIMMs)
MEM3640-4X32D=	Cisco 3640, 128 MB DRAM (4x32MB DRAM SIMMs)
MEM3660-32D=	Cisco 3660, 32 MB SDRAM Field Upgrade
MEM3660-128D=	Cisco 3660, 128 MB SDRAM Field Upgrade
MEM3660-2X64D=	Cisco 3660, 128 MB SDRAM (2x64 MB Flash DIMMs)
MEM3660-2X128D=	Cisco 3660, 256 MB Flash (2x128 MB Flash DIMMs)
BOOT-3600=	Boot ROM Upgrade for Cisco 3600

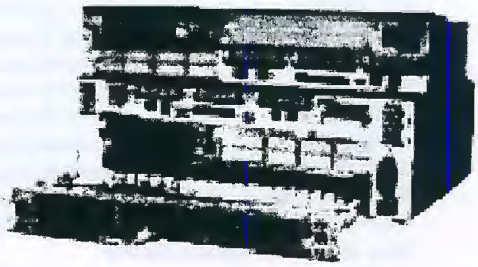
Cisco 3600 Series Accessories	
ACS-3620RM-19=	Cisco 3620—19-Inch Rack Mount Kit
ACS-3620RM-24=	Cisco 3620—24-Inch Rack Mount Kit
PWR-3620-AC	Cisco 3620—AC Power Supply
PWR-3620-DC	Cisco 3620—DC Power Supply
ACS-3620RPS=	Cisco 3620—RPS Field Upgrade
ACS-3640RM-19=	Cisco 3640—19-Inch Rack Mount Kit
ACS-3640RM-24=	Cisco 3640—24-Inch Rack Mount Kit
PWR-3640-AC	Cisco 3640—AC Power Supply
PWR-3640-DC	Cisco 3640—DC Power Supply
ACS-3640RPS=	Cisco 3640—RPS Field Upgrade
NM-BLANK-PANEL=	Blank Network Module Panel
WIC-BLANK-PANEL=	Blank WAN Interface Card Panel
ACS-3660RM-23	23 inch Rack Mount Kit for the Cisco 3660
PWR-3660-AC	AC Power Supply for Cisco 3660
PWR-3660-DC	DC Power Supply for Cisco 3660
Cisco 3600 Series Basic Packaged SMARTnet Maintenance 8x5xNBD	
CON-SNT-PKG7	Cisco 3620 Packaged SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG10	Cisco 3640 Packaged SMARTnetMaintenance 8x5xNBD
CON-SNT-PKG13	Cisco 3661 and Cisco 3662 Packaged SMARTnetMaintenance 8x5xNBD

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).
2. The ATM Modules, WAN Interface Card (WIC) Modules, Multiflex Voice/WAN Interface Cards, Voice/Fax Network Modules, High-Density Voice/Fax DSP Upgrade Modules, and Network Modules (International) for the 3600 series are the same as those for the 2600 series. Please see page 1-24 for part numbers.
3. Requires Plus feature pack.

For More Information

See the Cisco 3600 Series Web site: **http://www.cisco.com/go/3600**

Cisco 3700 Series



The Cisco 3700 Series is a new line of modular routers that enable flexible and scalable deployment of new applications in an integrated branch office access platform. The Cisco 3700 Series is ideal for sites and solutions requiring the highest levels of integration at the branch for branch office IP Telephony, voice gateway, and integrated flexible routing with low-density switching solutions.Integrated security, intrusion detection, and VPN protect the network at the perimeters, while integrated caching conserves WAN bandwidth. The Cisco 3700 Series provides a consolidated service infrastructure and high service density in a compact form factor that enables the incremental incorporation of branch applications.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 3725	• New levels of branch office service density in a compact form factor (2RU) • Integrated Security, intrusion detection, and VPN • Integrated flexble routing andlow-density switching (16-or-36 ports) • Flexible incrementaland scalable migration to a voice/data converged branch office network – Compatibility with more than 90% of the world's legacy analog and digtal TDM PBXs – Survivable Remote Site Telephony (SRST) features that enable centralized call processing with local branch IP Telephony redundancy – Inline power for IP Telephony • Content Networking and Caching integrated for WAN bandwidth conservation
Cisco 3745	Same features as above plus: • New levels of branch office service density in a compact formfactor (3RU) • Availability features such as redundant power, online insertion and removable components and field replaceable components • Increased performance and density

Key Features

- Optimized for multiple high density services
- Versatile High Density Service Module (HDSM) design enhances integrated services options
- Integrated connectivity options free up network module slots
- Optional features enhance availability/resiliency (3745 only): internal redundant power, hot-swappable modules, and field-serviceable components
- Optimized for Integrated IP Telephony: IP phone powered switch, high density voice gateway, flexible WAN routing, and Survivable Remote Site Telephony
- Flexible combination of analog and/or digital voice with scalable port density
- Full support for Cisco IOS voice suite of features
- Platforms performance-tuned for scaling packet voice solutions
- New integrated switching modules (16- and 36-port)
- Common user interface with Catalyst series switches
- Simplified management from a single platform for ease of configuration, deployment, and troubleshooting
- Integrated inline power for wireless access points and IP phones
- GigE connectivity

Specifications

Feature	Cisco 3725	Cisco 3745
Network Module Slots	2	4
Advanced Integration Module (AIM) Slots	2	2
WAN Interface Card (WIC) Slots	3	3
10/100 FE Ports	2	2
WAN Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
ATM Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Voice/Fax Network Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
WAN Interface Card (WIC) Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Multiflex Voice/WAN Interface Cards	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Voice Interface Card (VIC) Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Modem Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
EtherSwitch Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Performance	100 kpps	225 kpps
VPN/Security Advanced Integration Modules (AIM)	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Content Network Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Flash Memory	32 MB (default); 128 MB (max)	32 MB (default); 128 MB (max)
Flash Memory (External)	32 MB -128 MB (optional)	32 MB -128 MB (optional)
DRAM Memory	128 MB (default) 256 MB (max)	128 MB (default) 256 MB (max)
Power Supply	AC, DC optional	AC, DC optional
Dimensions (HxWxD)	3.5 x 17.25 x 14.7 in.	5.25 x 17.25 x 15 in.

Selected Part Numbers and Ordering Information[1]

Cisco 3700 SeriesModular Multiservice Access Router	
CISCO3725	2-slot Modular Multiservice Router with IP Sotware
CISCO3745	4-slot Modular Multiservice Router with IP Sotware
Serial Network Modules	
NM-4A/S	4-port async/sync serial network module
NM-8A/S	8-port async/sync serial network module
NM-1HSSI	1-port high speedserial interface module
Asynchronous Network Modules	
NM-16A	16 Async Ports network module
NM-32A	32 Async Ports network module
LAN Network Modules and Mixed-Media LAN & WAN Network Modules	
NM-2W	2 WAN Card Slot Network Module (no LAN)
NM-1FE2W	1 10/100 Ethernet2 WAN Card Slot Network Module
NM-1FE1R2W	1 10/100 Ethernet 1 4/16 Token Ring 2 WAN Card Slot NM
NM-2FE2W	2 10/100 Ethernet2 WAN Card Slot Network Module
NM-1FE-FX	1-port Fast Ethernet network module (10/100Base Fiber only)

Digital Packet Voice and Fax Trunk Network Modules

NM-HDV-1T1-12	High Density Voice Network Module, with 1 VWIC-1MFT-T1 and 1 PVDM-12
NM-HDV-1E1-12	High Density Voice Network Module, with 1 VWIC-1MFT-E1 and 1 PVDM-12
NM-HDV-1E1-30	Single-port, 30-channel E1 voice/fax Network Module (supports 30 channels) of medium complexity VoCoders: G.729a/b, G.726, G.711 and fax or 12 channels of G.726, G.729, G.723.1, G.728, G.729a/b, G.711 and fax)
NM-HDV-1E1-30E	Single-port, enhanced 30-channel E1 voice/fax Network Module (supports30 channels of high and medium complexity VoCoders: G.729a/b, G.726, G.729, G.728, G.723.1, G.711 and fax)
NM-HDV-2E1-60	Dual-port, 60-channel E1 voice/fax Network Module (supports 60 channels) of medium complexity VoCoders: G.729a/b, G.726,G.711and fax or 30channels of G726, G729, G723.1, G.728, G729a/b, G711 and fax) Supportsadd/drop multiplexing (drop andinsert)
NM-HDV-1T1-24	Single-port, 24-channel T1 voice/fax Network Module (supports 24 channels of medium complexity VoCoders: G.729a/b, G.726, G.711 and fax or 12 channels of G.726, G.729, G.723.1, G.728, G.729a/b, G.711 and fax)
NM-HDV-1T1-24E	Single-port, enhanced 24-channel T1 voice/fax Network Module (supports24 channels of high and medium complexity VoCoders: G.729a/b, G.726, G.729, G.728, G.723.1, G.711 and fax)
NM-HDV-2T1-48	Dual-port, 48-channel T1 voice/fax Network Module (supports 48 channels) of medium complexity VoCoders:G.729a/b,G.726,G.711 and fax or 24 channels of G726, G729, G723.1, G.728, G729a/b, G711 and fax) Supportsadd/drop multiplexing (drop andinsert)
AIM-ATM-VOICE-30	SAR and 30 Channel T1/E1 Digital Voice module
AIM-VOICE-30	30 Channel T1/E1 Digital Voice module

Analog Packet Voice and Fax Trunk Network Modules

NM-1V	1-slot voice and fax netwok module
NM-2V	2-slot voice and fax netwok module
NM-HDA	High Density Analog Module

Voice Interface Cards

VIC-2FXS	2-port voice interface card—FXS
VIC-2FXO	2-port voice interface card—FXO
VIC-2FXO-EU	2-port voice interface card—FXO (for Europe)
VIC-2FXO-M1	2-port voice interface card—FXO (with batteryreversal, for North America)
VIC-2FXO-M2	2-port voice interface card—FXO (with batteryreversal, for Europe)
VIC-2FXO-M3	2-port voice interface card—FXO (for Austelia)
VIC-2E/M	2-port voice interface card—E&M
VIC-2DID	2-port voice interface card—DID (Direct Inward Dial)
VIC-2BRI-S/T-TE	2-port voice interface card—BRI(Terminal side)
VIC-2BRI-NT/TE	2-port voice interface card—BRI (Network side)

ATM Network Modules

NM-4T1-IMA	4-port T1 ATM network module with Inverse Multiplexing over ATM (IMA)
NM-4E1-IMA	4-port E1 ATM network module with IMA
NM-8T1-IMA	8-port T1 ATM network module with IMA
NM-8E1-IMA	8-port E1 ATM network module with IMA
NM-1A-T3	1-port DS3 ATM network module
NM-1A-E3	1-port E3 ATM network module
AIM-ATM	ATM cell processing module

Serial WAN Interface Cards

WIC-1DSU-T1	One T1 CSU/DSU - Integrated
WIC-2T	2-port High Speed Serial
WIC-2-A/S	2-port Async/Sync Serial
WIC-1DSU-56K4	1-port, four-wire 56/64-Kbps with CSU/DSU

Digital Voice/WAN Interface Cards

VWIC-1MFT-T1	1-port RJ-48 MultiFlex Trunk—T1
VWIC-2MFT-T1	2-port RJ-48 MultiFlex Trunk—T1
VWIC-2MFT-T1-DI	2-port RJ-48 MultiFlex Trunk—T1 with Drop and Insert
VWIC-1MFT-E1	1-port RJ-48 MultiFlex Trunk—E1
VWIC-2MFT-E1	2-port RJ-48 MultiFlex Trunk—E1
VWIC-2MFT-E1-DI	2-port RJ-48 MultiFlex Trunk—E1 with Drop and Insert Add not for VWICs VIC slots & WIC slots
VWIC-1MFT-G703	1-port RJ-48 MultiFlex Trunk—E1 unstructured
VWIC-2MFT-G703	2-port RJ-48 MultiFlex Trunk—E1 unstructured

ISDN WAN Interface Cards

WIC-1B-S/T	1-port ISDN BRI
WIC-1B-U	1-port ISDN BRI with NT1

ISDN and Channelized Serial Network Modules	
NM-1CT1	1-port channelized T1/ISDN PRI network module
NM-1CT1-CSU	1-port channelized T1/ISDN PRI with CSU network module
NM-2CT1	2-port channelized T1/ISDN PRI network module
NM-2CT1-CSU	2-port channelized T1/ISDN PRI with CSU network module
NM-1CE1B	1-port channelized E1/ISDN PRI balanced networkmodule
NM-1CE1U	1-port channelized E1/ISDN PRI unbalancednetwork module
NM-2CE1B	2-port channelized E1/ISDN PRI balanced networkmodule
NM-2CE1U	2-port channelized E1/ISDN PRI unbalancednetwork module
NM-4B-S/T	4-port ISDN BRI network module
NM-4B-U	4-port ISDN BRI with NT1 networkmodule
NM-8B-S/T	8-port ISDN BRI network module (S/T interface)
NM-8B-U	8-port ISDN BRI with NT1 network module (U interface)
Modem Modules	
WIC-1AM	1-port analog modem WAN interface card (WIC)
WIC-2AM	2-port analog modem WAN interface card (WIC)
NM-6DM	6-port digital modem network module
NM-12DM	12-port digital modem networkmodule
NM-18DM	18-port digital modem networkmodule
NM-24DM	24-port digital modem networkmodule
NM-30DM	30-port digital modem networkmodule
NM-8AM	8-port analog modem Network Module
NM-16AM	16-port analog modem Network Module
NM-8AMJ	8-port analog modem Network Module—Japan
NM-16AMJ	16-port analog modem Network Module—Japan
Digital Subscriber Line (DSL)	
WIC-1ADSL	1-port ADSL WAN Interface Card
WIC-G.SHDSL	1-port G.shdsl WAN Interface Card
Encryption Advanced Integration Modules	
AIM-COMPR4	Data Compression AIM for 3660 Series (4 E1 performance)
AIM-VPN/HP	DES/3DES VPN Encryption AIMfor 3660-High Performance
AIM-VPN/EPDES/3DES	VPN Encryption AIM for 2600-Enhanced Performance
Content Engine Network Modules	
NM-CE-BP-20G-K9	Content EngineNetwork Module, Basic Performance, 20GB IDE Hard Disk
NM-CE-BP-40G-K9	Content EngineNetwork Module, Basic Performance, 40GB IDE Hard Disk
NM-CE-BP-SCSI-K9	Content Engine Network Module, Basic Performance, SCSI Controller
Dry Contact Closure Alarm NM	
NM-AIC-64	Alarm Monitoring and Control Network Module
Cisco EtherSwitch Modules	
NM-16ESW	One 16-Port 10/100 EtherSwitch Network Module
NM-16ESW-PWR	One 16 port 10/100 EtherSwitch NM with Inline Power support
NM-16ESW-1GIG	One 16 port 10/100 EtherSwitch NM with 1 GE (1000BaseT) port
NM-16ESW-PWR-1GIG	One 16 port 10/100 EtherSwitch NM withInline Power and GE
PPWR-DCARD-16ESW	One Inline power daughter card for16 port EtherSwitch NM
NMD-36-ESW	One 36 port 10/100 EtherSwitch High Density Service Module
NMD-36-ESW-PWR	One 36 port 10/100 EtherSwitch HDSM withInline Power
NMD-36-ESW-2GIG	One 36 port 10/100 EtherSwitch HDSM withtwo GE (1000BaseT)
NMD-36-ESW-PWR-2G	One 36 port 10/100 EtherSwitch HDSM+ Inline Power and two GE
PPWR-DCARD-36ESW	One Inline Power daughter card for 36 port EtherSwitch HDSM
GE-DCARD-ESW	One GE (1000BaseT) daughter card for EtherSwitch Modules
PPWR-PS-360W	One 48V (360W) power supply for EtherSwitch Modules
PPWR-PS-CHASSIS	One power supply chassis for Cisco 48V (360W) power supply
PWR-CHASSIS-360W	One power supply chassis and 48V power supply for EtherSwitch
CAB-PPWR-PS1-1	Connects one EtherSwitch power supply to one EtherSwitch Module
CAB-PPWR-PS1-2	Connects one EtherSwitch power supply to two EtherSwitch Modules
CAB-PPWR-PS2-1	Connects two EtherSwitch power supplies to one EtherSwitch Module

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the Distribution Product Reference Guide at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco 3600 Series Web site: **http://www.cisco.com/go/3700**

Cisco 7200 Series

The Cisco 7200 Series routers deliver exceptional price/performance, versatility, and feature-richness in a compact form factor. The Cisco 7200 is ideal as a WAN aggregator for the Service Provider (small POP) or enterprise edge, an enterprise WAN gateway, a high-end managed CPE, or as a small core router. The platform also supports sites that require IBM data center connectivity as well as sites that require multifunction capabilities that combine all the above for multiservice voice, video, and data traffic.

A key strength of the Cisco 7200 is its modularity. With a choice of 4- and 6-slot chassis, a selection of processors providing up to 1 Mpps, an extensive range of LAN and WAN interfaces with up to 48 ports per chassis, and single or dual power supplies, the customer can customize their system to achieve the performance, connectivity, and capacity desired. This modularity combined with a low initial price point guarantees both investment protection and maximum return on investment, allowing the customer to upgrade and/or redeploy their Cisco 7200 as their network needs change.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7204VXR	• 4-slot chassis • Modular processor: 225, 400, 900 Kpps (NPE-225, NPE-400, NPE-G1) or 300 Kpps service accelerator (NSE-1) • 1.2 Gbps backplane • MIX-enabled busfor data/voice/video applications
Cisco 7206VXR	• 6-slot chassis • Modular processor: 225, 400, 900 Kpps (NPE-225, NPE-400, NPE-G1) or 300 Kpps service accelerator (NSE-1) • 1.2 Gbps backplane • MIX-enabled busfor data/voice/video applications

Key Features

- Compact Form Factor—Up to six port adapters in a fully modular 3RU form factor. The optional Rack Density System (RDS) allows for up to nine Cisco 7206 routers per rack with front-to-back airflow
- Exceptional Value—As the most powerful single-processor platform, the Cisco 7200 offers customers a superior price/performance ratio supporting high-speed media and high-density configurations with up to 900 Kpps processing at a competitive price point
- Feature Rich—Full support for Cisco IOS software and enhancements for high-performance network services enables the Cisco 7200 to offer industry-leading network services, including: MPLS, broadband aggregation, quality of service (QoS), security, and voice/video/data support
- Connectivity/Flexibility—Provides high port density and an extensive range of LAN and WAN media, the Cisco 7200 dramatically reduces the cost per port and allows for flexible configurations to meet your specific network needs
- Common port adapters—Port adapters are shared with the Cisco 7300, 7400, 7500, and 7600 (w/FlexWAN Module), which simplifies sparing and protects customer investment in interfaces

Competitive Products

- Redback: SMS-500, SMS-1800
- Juniper: M5, M10
- Unisphere: ERX700, ERX1400

Specifications

Feature	Cisco 7204VXR	Cisco 7206VXR
Fixed Ports	None	Same as 7204VXR
Expansion Slots	4	6
WAN Port Adapters	DS0 to OC-12	Same as 7204VXR
Processor	RM7K RISC Processor with optional PXF Processor	Same as 7204VXR
Forwarding Rate	Up to 1 Mpps	Same as 7204VXR
Backplane Capacity	1.2 Gbps	Same as 7204VXR
Flash PCMCIA Memory	48 MB (expandable to 256 MB)	Same as 7204VXR
System DRAM Memory	128 MB (expandableto 1 GB)	Same as 7204VXR
Minimum Cisco IOS Release	12.0(1)XE	Same as 7204VXR
Internal Power Supply	AC or DC, dual option	Same as 7204VXR
Redundant Power Supply	Yes, for AC or DC	Same as 7204VXR
Chassis Height	3 RU	Same as 7204VXR
Rack Mountable	Yes, up to 16 per rack	Same as 7204VXR
Dimensions (HxWxD)	5.25 x 16.8 x 17 in.	Same as 7204VXR

Cisco IOS Software and Memory Requirements[1]

To run the Cisco IOS Feature Packs, you need, at a minimum, the amount of memory shown in the following table. Some configurations will require more.

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required	DRAM Memory Required
CD72-C-12.1T=	IP	12.1T	16MB	64MB
CD72-CK2-12.1E=	IP IPSEC 3DES	12.1E	16MB	64MB
CD72-CHK2-12.1T=	IP/FW/IDS IPSEC 3DES	12.1T	16MB	64MB
CD72-A-12.1T=	Enterprise	12.1T	16MB	64MB

[1] For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information." For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

Selected Part Numbers and Ordering Information[1]

Cisco 7204 Chassis	
CISCO7204VXR	Cisco 7204VXR, 4-slot chassis, 1 AC Supply w/IP Software
CISCO7204VXR/225	7204VXR Bundle with NPE-225 and I/O Controller with 2 FE/E
Cisco 7206 Chassis	
CISCO7206VXR	Cisco 7206VXR, 6-slot chassis, 1 AC Supply w/IP Software
C7206VXR/400/2FE	7206VXR with NPE-400 and I/O Controller with 2 FE/E Ports
C7206VXR/400/GE	7206VXR with NPE-400 and GE+E I/O controller
7206VXR/NPE-G1	7206VXR with NPE-G1 processing engine
Cisco 7200 CPE Bundles	
7204VXR/CPE	7204VXR w/ NPE-225, 2 FE I/O, choice of specfied WAN PA
Cisco 7200 Voice Bundles	
C7206VXR/VOICE/400	7206VXR w/ NPE-400, Voice PA PA-VXC-2TE1+, I/O contlr w/ 2FE
Cisco 7200 VPN Bundle	
7204VXR/VPN/400K9	7204VXR VPN Bundle NPE400,128MB, I/O 2FE, ISA,IPSEC 3DES IOS
7204VXR400/VPNK9	7204VXR VPN Bundle NPE400,128MB, I/O 2FE, VAM,IPSEC 3DES IOS
7204VXR225/VPNK9	7204VXR VPN Bundle NPE225,128MB, I/O 2FE, VAM,IPSEC 3DES IOS
7206VXR400/VPNK9	7206VXR VPN Bundle NPE400,256MB, I/O 2FE, VAM,IPSEC 3DES IOS
7206VXRG1/VPNK9	7206VXR VPN Bundle NPE-G1,256MB, 3 FE/GE, VAM,IPSEC 3DES IOS

Cisco 7200 Series Processors

NPE-G1=	Cisco 7200 Network Processing Engine NPE-G1 including 256MB defaultDRAM and 64MB default flash memory.
NPE-225=	Network Processing Engine 225 (128MB default memory)-spare
NPE-400=	7200VXR NPE-400 (128MB default memory),SPARE
NSE-1=	7200VXR Network Services Engine 1 (128MB default mem),SPARE

Cisco 7200 Series Input/Output Controller

C7200-I/O=	Cisco 7200 Input/Output Contoller, Spare
C7200-I/O-2FE/E=	Cisco 7200 Input/Output Controller with Dual 10/100 Ethernet
C7200-I/O-GE+E=	Cisco 7200 Input/Output Controller with GE and Ethernet

Cisco 7200 Rack Mount Systems

CISCO7200RDS	CISCO 7200 Rack Density System

Cisco 7200 Processor Memory: NPE-G1

MEM-NPE-G1-256MB=	Two 128MB memory modules (256MB total) for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-512MB=	Two 256MB memory modules (512MB total) for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-1GB=	Two 512MB memory modules (1GB total) for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-FLD64=	64MB Compact Flash Disk for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-FLD128=	128MB Compact Flash Disk for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-FLD256=	256MB Compact Flash Disk for the Cisco 7200 Network Processing Engine NPE-G1

Cisco 7200 Processor Memory: NPE-100, NPE-150, NPE-200

MEM-NPE-16MB=	16MB Memory Upgrade Kit for NPE-200/NPE-150/NPE-100
MEM-NPE-32MB=	32MB Memory Upgrade Kit for NPE-200/NPE-150/NPE-100
MEM-NPE-64MB=	2 32MB memory modules(64MB total) forNPE-200/NPE-150/NPE-100
MEM-NPE-128MB=	128MB Memory Upgrade Kit for NPE-200/NPE-150/NPE-100

Cisco 7200 Processor Memory: NPE-175 and NPE-300

MEM-SD-NPE-32MB=	32MB Memory Upgrade Kit for NPE-300/NPE-225/NPE-175
MEM-SD-NPE-64MB=	64MB Memory Upgrade Kit for NPE-300/225/175
MEM-SD-NPE-128MB=	128MB Memory Upgrade Kit for NPE-300/NPE-225/NPE-175
MEM-SD-NPE-256MB=	2 128MB memory modules (256MB total) for the NPE-300 in 7200

Cisco 7200 Processor Memory: NPE-225 and NSE-1

MEM-SD-NPE-128MB=	128MB Memory Upgrade Kit for NPE-300/NPE-225/NPE-175
MEM-SD-NSE-256MB=	256MB Memory for NPE-225 or NSE-1 in 7200 Series, SPARE

Cisco 7200 Processor Memory: NPE-400

MEM-NPE-400-128MB=	128MB Memory for NPE-400 in 7200 Series
MEM-NPE-400-256MB=	256MB Memory for NPE-400 in 7200 Series
MEM-NPE-400-512MB=	512MB Memory for NPE-400 in 7200 Series

Cisco 7200 Series Input/Output Controller Memory Options

MEM-CIP-32M=	CIP 32 MB DRAM Upgrade Kit
MEM-CPA-32M=	CPA 32MB DRAM Upgrade Kit
MEM-I/O-FLC20M=	Cisco 7200 I/O PCMCIA Flash Memory, 20MB
MEM-I/O-FLC8M=	Cisco 7200 I/O PCMCIA Flash Memory, 8MB
MEM-I/O-FLD128M=	Cisco 7200 I/O PCMCIA Flash Disk, 128 MB Spare
MEM-I/O-FLD48M=	Cisco 7200 I/O PCMCIA Flash Disk, 48 MB Spare

Cisco 7200 Series Port Adapters

PA-4C-E=	1 Port Enhanced ESCON Channel Port Adapter
PA-A2-4E1XC-E3ATM=	CES Port Adapter E3/E1 120 ohms
PA-A2-4E1XC-OC3SM=	CES OC3 Port Adapter4E1 Ports 120ohms
PA-A2-4T1C-OC3SM=	ATM CES Port Adapter, 4T1 CES Portsand 1 OC3 ATM SM Port
PA-A2-4T1C-T3ATM=	ATM CES Port Adapter, 4T1 CES Ports and 1 T3 ATM Port
PA-GE=	Gigabit Ethernet Port Adapter
PA-MCX-2TE1=	Spare 2 port MIX-enabled multichannel T1/E1 PA with CSU/DSU
PA-MCX-4TE1=	4 port MIX-enabled multichannelT1/E1 PA with CSU/DSU
PA-MCX-8TE1-M=	T1/E1 SS7 link PA for ITP
PA-MCX-8TE1=	8 port MIX-enabled multichannel T1/E1 with CSU/DSU
PA-SRP-OC12MM=	DPT-OC12 Multi-mode port adapter
PA-SRP-OC12SMI=	DPT-OC12 Single-mode intermediate port adapter
PA-SRP-OC12SML=	DPT-OC12 Single-mode long-reachport adapter
PA-SRP-OC12SMX=	DPT-OC12 Singe-mode extended reach PA

Cisco 7200, 7400 and 7500 Series Port Adapters

PA-VXC-2TE1+=	2 port TE1 hi-capacity enhanced voice PA
PA-VXB-2TE1+=	2 port T1/E1 moderate capacity enhanced voice PA
PA-T3=	1 Port T3 Serial Port Adapterwith T3 DSUs
PA-T3+=	1 Port T3 Serial Port Adapter Enhanced
PA-POS-OC3SML=	1-Port Packet/SONET OC3c/STM1 Singlemode (LR) PA
PA-POS-OC3SMI=	1-Port Packet/SONET OC3c/STM1 Singlemode (IR) PA
PA-POS-OC3MM=	1-Port Packet/SONET OC3c/STM1 Multimode PA
PA-POS-2OC3=	2 Port Packet/SONET OC3c/STM1 Port Adapter
PA-MC-T3=	1 port multichannel T3port adapter
PA-MC-E3=	1 port Multi-Channel E3port adapter
PA-MC-4T1=	4 port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-2T3+=	2 port multichannel T3port adapter
PA-MC-2T1=	2 port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-2E1/120=	2 port multichannel E1 port adapter with G.703 120ohm interf
PA-H=	Port Adapter: 1-Port HSSI
PA-E3=	1 Port E3 Serial Port Adapterwith E3 DSU
PA-A3-T3=	1-Port ATM Enhanced DS3Port Adapter (Spare)
PA-A3-OC3SML=	1-Port ATM Enhanced OC3c/STM1 Singlemode(LR)Port Adapter
PA-A3-OC3SMI=	1-Port ATM Enhanced OC3c/STM1 Singlemode(IR)Port Adapter
PA-A3-OC3MM=	1-Port ATM Enhanced OC3c/STM1 Multimode Port Adapter
PA-A3-E3=	1-Port ATM Enhanced E3 Port Adapter (Spare)
PA-A3-8E1IMA=	8-port ATM Inverse Mux E1 (120 Ohm) Port Adapter, Spare
PA-8T-X21=	8-Port Serial, X.21 Port Adapter
PA-8T-V35=	8-Port Serial, V.35 Port Adapter
PA-8T-232=	8-Port Serial, 232 Port Adapter
PA-8E=	8-Port Ethernet 10BaseT Port Adapter
PA-4T+=	4-Port Serial Port Adapter, Enhanced
PA-4E1G/75=	4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
PA-4E1G/120=	4-Port E1 G.703 Serial Port Adapter (120ohm/Balanced)
PA-4E=	4-Port Ethernet 10BaseT Port Adapter
PA-2T3=	2 Port T3 Serial Port Adapterwith T3 DSUs
PA-2T3+=	2 Port T3 Serial Port Adapter Enhanced,Spare
PA-2H=	PORT ADAPTER:2-PORT HSSI
PA-2FE-TX=	2-Port Fast Ethernet 100Base TX Port Adapter
PA-2FE-FX=	2-Port Fast Ethernet 100Base FX Port Adapter
PA-2E3=	2 Port E3 Serial Port Adapterwith E3 DSUs

Cisco 7200 and 7400 Series Port Adapters

PA-8B-S/T=	8-Port BRI Port Adapter, S/T Interface

Cisco 7200 and 7500 Series Port Adapters

PA-VXA-1TE1-30+=	1 Port T1/E1 Digital Voice Port Adapterwith 30 Channels
PA-VXA-1TE1-24+=	1 Port T1/E1 Digital Voice Port Adapterwith 24 Channels
PA-MC-STM-1SMI=	1 port multichannel STM-1 single mode port adapter
PA-MC-STM-1MM=	1 port multichannel STM-1multimode port adapter
PA-MC-8TE1+=	8 port multichannel T1/E1 8PRI port adapter
PA-F/FD-SM=	1-Port FDDI Full Duplex Single-Mode Port Adapter
PA-F/FD-MM=	1-Port FDDI Full Duplex Multi-Mode Port Adapter
PA-A3-8T1IMA=	8-port ATM Inverse Mux T1 Port Adapter, Spare
PA-4R-DTR=	Port Adapter:4-Port Dedicated Token Ring,4/16Mbps, HDX/FDX

Cisco 7200 Series Service Adapters

SA-ISA=	Integrated Services Adapter for IPSec or MPPE encryption
SA-VAM=	VPN Acceleration Module (VAM)IPSec and IPComp Acceleration

Cisco 7200 Series Transceiver Modules

GBIC-LX/LH=	Gigabit Interface Converterfor 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. Converter for 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX
POM-OC3-MM	1-port OC3/STM1 Pluggable Optic Module,MM
POM-OC3-SMIR	1-port OC3/STM1 Pluggable Optic Module, SM-IR
POM-OC3-SMLR	1-port OC3/STM1 Pluggable Optic Module, SM-LR

Cisco 7200 Series Power Supplies	
PWR-7200-DC+=	Cisco 7200 DC (24V-60V) Power Supply Option
PWR-7200/2-DC+	Cisco 7200 Dual DC (24V-60V) Power Supply Option
PWR-7200-AC=	Cisco 7200 AC Power Supply With United States Cord
PWR-7200-ACA=	Cisco 7200 AC Power Supply With Australian Cord
PWR-7200-ACE=	Cisco 7200 AC Power Supply With European Cord
PWR-7200-ACI=	Cisco 7200 AC Power Supply With Italian Cord
PWR-7200-ACU=	Cisco 7200 AC Power Supply With United Kingdom Cord
Cisco 7200 Series Spares and Accessories	
ACS-7200-RMK=	Cisco 7200 Rackmount Kit and Cable Management Bracket
CVPN7200FIPS/KIT=	Kit(Instructions,labels)to configure 7206 for FIPS operation

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 7200 Series Web site: **http://www.cisco.com/go/7200**

Cisco 7300 Series

The Cisco 7300 Series Routers are optimized for flexible, high performance IP/MPLS services at the network edge, where service providers and enterprises link together. Coupled with powerful network processing, a broad set of interfaces and a compact, modular form factor the Cisco 7300 Series Routers are ideal for intelligent, multi-gigabit network connectivity.

The Cisco 7304 Series Router is ideally applied as a high-end CPE or as an Internet Gateway router. Architected for network High Availability and multi-protocol support, the 7304 supports the broad set of existing Cisco 7000 Series Port Adapters with the new Cisco 7304 Port Adapter Carrier Card.

The Cisco 7301 Series Router is a compact single rack unit router coupled with a broad set of interfaces and Cisco IOS software features. It packs high performance in a space and power efficient form factor that includes a single 7000 Series port adapter slot, 3 on-board Gigabit Ethernet (copper or optical)/Fast Ethernet ports and a new high-speed bus technologies.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7301	• Compact, powerefficient 1RU form factor • Three times the performance increase over existing single rack unit routers like the Ciso 7401 • Single 7000 Series Port Adapter Slot
Cisco 7304	• Highly modular price and performance optmized platform, rich in IP services • High performance connectivity—DS-1 through OC48/STM16 with 3.5 Mpps performance • Built-in Gigabit Ethernet connectivity • Multiprotocol routing:IP, IPX, AppleTalk, DLSw • Compact size, high availability and optimal cooling

Key Features

- Cisco 7301: With nearly 1 million-packets-per-second (Mpps) processing performance, the fastest Cisco 1RU general-purpose processor, as of January 2003; 3 fixed 10/100/1000-Mbps ports (RJ-45 or SFP optics) directly on the processor; Full Cisco IOS feature support; Pluggable Gigabit Ethernet optics (SFPs); Up to 1GB of available DRAM; Up to 256MB of removable compact flash memory; Front-back airflow and single sided management
- Cisco 7304: Compact modular form factor with four RU with four port adapter slots per chassis; PXF IP processor hardware-accelerated services such as Cisco Express Forwarding (CEF), NetFlow v8, and Turbo ACL; Offers 3.5Mpps performance for PXF-accelerated services with the NSE-100 Network Services Forwarding Engine; Two Gigabit Ethernet ports per NSE-100; System redundancy: optional dual processors and dual AC or DC power supplies increases network availability

Competitive Products

- Redback: SMS-500, SMS-1800
- Juniper: M5, M10
- Unisphere: ERX700, ERX1400

Specifications

Feature	Cisco 7301	Cisco 7304
Fixed Ports	Three Gigabit Ethernet ports	Same as 7301
Expansion Slots	1	4
WAN Interface Range	DS-1 to OC-3	T3 to OC-48
Processor	RM 7000 MIPS Processor + PXF Processor	RM 7000 MIPS Processor + PXF Processor
Forwarding Rate	Up to 1 Mpps	Up to 3.5 Mpps
Backplane Capacity	1.2 Gbps	16 Gbps
Flash PCMCIA Memory	64 MB (expandable to 128 MB)	Same as 7301
System DRAM Memory	128 MB (expandableto 512 MB)	Same as 7301
Minimum Cisco IOS Release	12.2(11)YZ	12.1(9)EX
Internal Power Supply	AC or DC	Same as 7301
Redundant Power Supply Support	Yes, for AC or DC	Same as 7301
Chassis Height	1 RU	4 RU
Rack Mountable	Yes, up to 40 per rack	Yes, up to 11 per rack
Dimensions (HxWxD)	1.73 x 17.3 x 13.87 in.	7 x 17.2 x 20.5 in.

Selected Part Numbers and Ordering Information[1]

Cisco 7300 System

PWR-7301-AC	Cisco 7301 AC Power Supply Option
PWR-7301/2-AC	Cisco 7301 Dual AC Power Supply Option
PWR-7301-DC48	Cisco 7301 DC48 Power Supply Option
PWR-7301/2-DC48	Cisco 7301 Dual DC48 Power Supply Option
PWR-7301-DC24	Cisco 7301 DC24 Power Supply Option
CISCO7301	Cisco 7301 chassis, 256MB memory, A/C power,64MB Flash
CISCO7304=	Cisco 7300, 4-slot chassis
CISCO7304-CH	Cisco7304 channel bundle
7300-NSE-100=	Cisco 7304 Network Services Engine 100
7300-NSE-100/2	Redundant Cisco 7304 NSE-100 w/Redundancy Feature License
7300-PWR-DC=	Cisco 7304 DC Power Supply Spare
7300-PWR-AC=	Cisco 7304 AC Power Supply Spare
7300-PWR/2-DC	Cisco 7304 Redundant DC Power Supply Option
7300-PWR/2-AC	Cisco 7304 Redundant AC Power Supply Option

Cisco 7300 Memory Options

MEM-7301-1GB=	1GB memory upgrade for 7301
MEM-7301-512MB=	512MB memory upgrade for 7301
MEM-7301-256MB=	256MB memory upgrade for Cisco 7301
7300-MEM-128=	128MB default SDRAM for 7304 NSE-100, spare
7300-MEM-256=	256MB SDRAM for 7304 NSE-100, spare
7300-MEM-512=	512MB SDRAM for 7304 NSE-100, spare
7300-I/O-CFM-64M=	Cisco 7304 Compact Flash Memory, 64 MB
7300-I/O-CFM-128M=	Cisco 7304 Compact Flash Memory, 128 MB

Cisco 7300 Series Compact Flash Disk Options

MEM-7301-FLD64=	Compact Disk Flash for 7301,64MB option
MEM-7301-FLD128=	Compact Disk Flash for 7301, 128MB option
MEM-7301-FLD256	Compact Disk Flash for 7301, 256MB Option

Cisco 7300 Line Cards

7300-1OC12POS-MM=	1-port OC12 POS line card for Cisco7304 w/ Multi-mode
7300-1OC12POS-SMI=	1-port OC12 POS line card for Cisco 7304 w/ Single-mode IR
7300-1OC12POS-SML=	1-port OC12 POS line card for Cisco 7304 w/ Single-mode LR
7300-1OC48POS-SMI=	1-port OC48 POS line card for Cisco 7304 w/ Single-mode IR
7300-1OC48POS-SML=	1-port OC48 POS line card for Cisco 7304 w/ Single-mode LR
7300-1OC48POS-SMS=	1-port OC48 POS line card for Cisco 7304 w/ Single-mode SR
7300-2OC12POS-MM=	2-port OC12 POS line card for Cisco7304 w/ Multi-mode
7300-2OC12POS-SMI=	2-port OC12 POS line card for Cisco 7304 w/ Single-mode IR
7300-2OC12POS-SML=	2-port OC12 POS line card for Cisco 7304 w/ Single-mode LR
7300-2OC3ATM-MM=	2-port OC3 ATM line card for Cisco 7304 w/ Multi-mode
7300-2OC3ATM-SMI=	2-port OC3 ATM line card for Cisco 7304 w/ Single-mode IR
7300-2OC3ATM-SML=	2-port OC3 ATM line card for Cisco 7304 w/ Single-mode LR
7300-2OC3POS-MM=	2-port OC3 POS line card for Cisco 7304 w/ Multi-mode
7300-2OC3POS-SMI=	2-port OC3 POS line card for Cisco 7304 w/ Single-mode IR
7300-2OC3POS-SML=	2-port OC3 POS line card for Cisco 7304 w/ Single-mode LR
7300-4OC3POS-MM=	4-port OC3 POS line card for Cisco 7304 w/ Multi-mode
7300-4OC3POS-SMI=	4-port OC3 POS line card for Cisco 7304 w/ Single-mode IR
7300-4OC3POS-SML=	4-port OC3 POS line card for Cisco 7304 w/ Single-mode LR
7300-6T3=	6-port T3 line card for Cisco 7304 w/ DSU

Cisco 7300 Series Transceiver Modules

GBIC-LX/LH=	Gigabit Interface Converter for 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. ConverterFor 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX

Cisco 7300 Accessories

7300-HALFSLOTBLNK	Cisco 7304 Half Slot Blank Line Card
7300-4RU/RCKBRKT=	Cisco 7304 Chassis Rackmount Bracket Spare
7300-CNTR-SPTUM=	Cisco 7304 Center Septum Spare

Cisco 7300 Software Options

S73A-12215B=	Cisco 7301 Series IOS ENTERPRISE
S73AH-12215B=	Cisco 7301 Series IOS ENTERPRISE/FW/IDS
S73AHK8-12215B=	Cisco 7301 Series IOS ENTERPRISE/FW/IDS IPSEC 56
S73AHK9-12215B=	Cisco 7301 Series IOS ENTERPRISE/FW/IDS IPSEC 3DES
S73AS-12215B=	Cisco 7301 Series IOS ENTERPRISE SSG
S73C-12215B=	Cisco 7301 Series IOS IP
S73A-12211YZ=	Cisco 7300 Series IOS ENTERPRISE
S73C-12211YZ=	Cisco 7300 Series IOS IP PLUS
S730A-12211YZ=	Cisco 7301 Series IOS ENTERPRISE
S730C-12211YZ=	Cisco 7301 Series IOS IP
S730Z-12211YZ=	Cisco 7301 Series IOS SERVICE PROVIDER
S73A-12113EX=	Cisco 7300 IOS ENTERPRISE
S73AHK2-12113EX=	Cisco 7300 IOS ENTERPRISE/FW/IDS IPSEC 3DES
S73AHL-12113EX=	Cisco 7300 IOS ENTERPRISE/FW/IDS IPSEC 56
S73AR1P-12113EX=	Cisco 7300 IOS CISCO 7300 SERIES IOS ENTERPRISE/SNASW PLUS
S73CHK2-12113EX=	Cisco 7300 IOS IP/FW/IDS IPSEC 3DES
S73CHL-12113EX=	Cisco 7300 IOS IP/FW/IDS IPSEC 56
S73CP-12113EX=	Cisco 7300 IOS IP PLUS
S73A-12112EX=	Cisco 7300 IOS ENTERPRISE
S73AHK2-12112EX=	Cisco 7300 IOS ENTERPRISE/FW/IDS IPSEC 3DES
S73AHL-12112EX=	Cisco 7300 IOS ENTERPRISE/FW/IDS IPSEC 56
S73AR1P-12112EX=	Cisco 7300 IOS CISCO 7300 SERIES IOS ENTERPRISE/SNASW PLUS
S73CHK2-12112EX=	Cisco 7300 IOS IP/FW/IDS IPSEC 3DES
S73CHL-12112EX=	Cisco 7300 IOS IP/FW/IDS IPSEC 56
S73CP-12112EX=	Cisco 7300 IOS IP PLUS

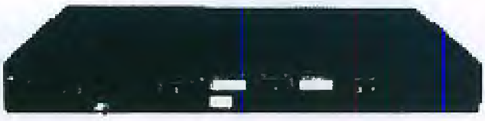
Cisco 7300 Carrier Cards	
7300-CC-PA=	7304 Carrier Card for 7200 Series Port Adapters
SFPs for Cisco 7301 Series	
GLC-SX-MM=	GE SFP, LC connector SXtransceiver
GLC-LH-SM=	GE SFP, LC connector LHtransceiver

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 7300 Series Web site: **http://www.cisco.com/go/7300**

Cisco 7400 Series



With the Cisco 7400, this modular, one-port adapter slot unit leverages over 40 standard 7200/7500 series port adapters. Its compact, stackable architecture is designed for application specific routing deployments, such as broadband services aggregation (PPP/L2TP) and WAN edge connectivity in service provider and enterprise networks. Leveraging Cisco patented technology, the Cisco 7400 series delivers a premium suite of hardware-accelerated network services.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7401ASR-CP	• General WAN edge connectivity in a small form factor, or as managed customer premise equipment (CPE) • Broad range of connectivity options—from DS0 to OC-3 interfaces • Comprehensive management services with remote management, provisioning, trouble shooting and software upgrade • Hardware accelerated services, including: NAT, ACLs, Netflow, CBWFQ, CBWRED, Policing, marking, Hierarchical Traffic Shaping, & VRF lite
Cisco 7401ASR-BB	• Complete broadbandsubscriber services suite with highest subscribers per rack ratio • One fast LAN interface (FE/GE) and one fast WAN interface (DS3/OC3) • High volume/densityof PPP, PPPoE, PPPoA, L2TP tunnel aggregation and termination for broadband services like DSL, Cable, and Wireless

Key Features

- Compact form factor with 1 RU, front-to-back airflow and stackability
- Hardware—accelerated IP network services
- Built-in dual GE connectivity
- Flexible WAN connectivity supporting over 40 interfaces including serial, multichannel, ISDN, Frame Relay, ATM, Packet over SONET (POS), from NxDS0 to OC-3
- Shared port adaptors with the Cisco 7200, 7300, 7500, and 7600 (with FlexWAN Module), which simplifies sparing and protects customer investment in interfaces

Competitive Products

- Redback: SMS500, SMS1800
- Juniper: M5, M10
- Unisphere: ERX700, ERX1400

Specifications

Feature	Cisco 7401ASR-BB	Cisco 7401ASR-CP
Fixed Ports	2 Gigabit Ethernet (RJ or GBIC) ports	Same as 7401ASR-BB
Expansion Slots	1	Same as 7401ASR-BB
WAN Interface Range	DS0 to OC-3	Same as 7401ASR-BB
Processor	RM7K RISC Processor + PXF Processor	Same as 7401ASR-BB
Forwarding Rate	Up to 350 Kpps	Same as 7401ASR-BB
Backplane Capacity	1.2 Gbps	Same as 7401ASR-BB
Flash PCMCIA Memory	64MB (expandable to 128MB)	Same as 7401ASR-BB
System DRAM Memory	256MB (expandable to512MB)	128MB (expandable to 512MB)
Minimum Cisco IOS Release	12.2(1)DX	Same as 7401ASR-BB
Internal Power Supply	AC, DC48V, DC24V, or Dual DC48V	Same as 7401ASR-BB
Redundant Power Supply Support	Yes	Same as 7401ASR-BB
Chassis Height	1 RU	Same as 7401ASR-BB
Rack Mountable	Yes, up to 40 per rack	Same as 7401ASR-BB
Dimensions (HxWxD)	1.72 x 17.3 x 11.80 in	Same as 7401ASR-BB

Selected Part Numbers and Ordering Information[1]

Cisco 7400 ASR Bundles	
CISCO7401ASR-BB	7401ASR, 256M SDRAM, Broadband Feature License
CISCO7401ASR-CP	7401ASR,128M SDRAM, IP Software
CISCO7401-2DC48=	Cisco 7400 chassis with dual DC power supply
7401ASR-CPT3	7401ASR,256M SDRAM, PA-T3+
C7400VPN/K9	7400 VPNRouter w/VAM,VPN DeviceMgr, 2xFE/GE,AC PS,IPSEC 3DES
Cisco 7400 ASR Memory Options	
MEM-COMP-FLD64M=	Cisco 7400ASR Compact Flash Disk, 64 MB (spare)
MEM-COMP-FLD128M=	Cisco 7400ASR Compact Flash Disk, 128 MB (spare)
MEM-7400ASR-256MB=	256MB Spare memory for Cisco 7400ASR/VPN
MEM-7400ASR-512MB=	512MB Spare SDRAM for Cisco 7400ASR/VPN
Cisco 7400 ASR Transceiver Modules	
GBIC-LX/LH=	Gigabit Interface Converterfor 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. ConverterFor 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX
POM-OC3-MM	1-port OC3/STM1 Pluggable Optic Module,MM
POM-OC3-SMIR	1-port OC3/STM1 Pluggable Optic Module, SM-IR
POM-OC3-SMLR	1-port OC3/STM1 Pluggable Optic Module, SM-LR
Cisco 7400 and 7500 Series Port Adapters	
PA-POS-OC3MM=	1-Port Packet/SONET OC3c/STM1 Multimode PA
PA-MC-8E1/120=	8 port multichannel E1 port adapter with G.703 120ohm interf
PA-2FE-FX=	2-Port Fast Ethernet 100Base FX Port Adapter
Cisco7200, 7400 and 7500 Series Port Adapters[2]	
Cisco 7400 ASR Power Supplies and Cords	
CAB-AC=	AC Power Cord, US
CAB-ACA=	AC Power Cord, Australia
CAB-ACE=	AC Power Cord, Europe
CAB-ACI=	AC Power Cord, Italy
CAB-ACR=	Power Cord Argentina, Spare
CAB-ACU=	AC Power Cord, UK
Cisco 7400 Software Options	
S74CHK9-12209YE=	Cisco 7400 Series IOS IP/FW/IDS IPSEC 3DES
S74CK9-12209YE=	Cisco 7400 Series IOS IP PLUS IPSEC 3DES
S74A-12204B=	Cisco 7400 Series IOS ENTERPRISE
S74AH-12204B=	Cisco 7400 Series IOS ENTERPRISE/FW/IDS
S74AHK9-12204B=	Cisco 7400 Series IOS ENTERPRISE/FW/IDS IPSEC 3DES
S74AS-12204B=	Cisco 7400 Series IOS ENTERPRISE SSG
S74C-12204B=	Cisco 7400 Series IOS IP
S74A-12202DD=	Cisco 7400 Series IOS ENTERPRISE
S74AH-12202DD=	Cisco 7400 Series IOS ENTERPRISE/FW/IDS

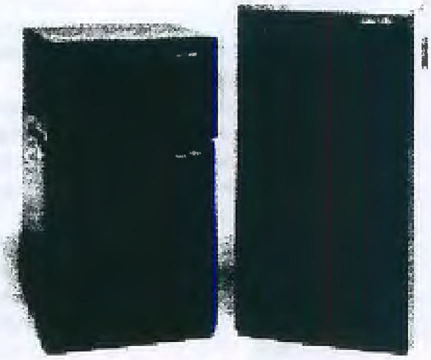
Cisco 7400 VPN Memory Options	
MEM-COMP-FLD64M=	Cisco 7400ASR Compact Flash Disk, 64 MB (spare)
MEM-COMP-FLD128M=	Cisco 7400ASR Compact Flash Disk, 128 MB (spare)
MEM-7400ASR-256MB=	256MB Spare memory for Cisco 7400ASR/VPN
MEM-7400ASR-512MB=	512MB Spare SDRAM for Cisco 7400ASR/VPN
Cisco 7400 VPN Transceiver Modules	
GBIC-LX/LH=	Gigabit Interface Converterfor 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. Converter for 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX
Cisco 7400 VPN Power Supplies and Cords	
CAB-AC=	AC Power Cord, US
CAB-ACA=	AC Power Cord, Australia
CAB-ACE=	AC Power Cord, Europe
CAB-ACI=	AC Power Cord, Italy
CAB-ACR=	Power Cord Argentina,Spare
CAB-ACU=	AC Power Cord, UK

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.
2. Cisco 7200, 7400 and 7500 share many port adapters. Please see Cisco 7200, 7400 and 7500 Series Port Adapters, page 1-34 for additional part numbers.

For More Information

See the Cisco 7400 Series Web site: **http://www.cisco.com/go/7400**

Cisco 7500 Series



An essential part of both Enterprise and Service Provider networks, the Cisco 7500 Series routers are the market leader for edge applications, due to its breadth of services, diverse interfaces, reliability, and performance. Since its inception, the Cisco 7500 has seen huge improvements in performance and its ability to scale, most recently with the Route Switch Processor 16 (RSP16) and Versatile Interface Processor 6-80 (VIP6-80) module. This series combines Cisco's proven software technology with exceptional reliability, availability, serviceability, and performance features to meet the requirements of today's most mission-critical networks.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7505	• 5 expansion slots • One CyBus • DS0 to OC-12 connectivity(all platforms)
Cisco 7507	• 7 expansion slots • Dual CyBuses • Redundant powersupplies • Diverse set of routingprotocols (allplatforms)
Cisco 7513	• 13 expansion slots • Dual CyBuses • Redundant powersupplies • Diverse set of routingprotocols (allplatforms)

Key Features

- High-performance switching—Delivers high performance for mission-critical applications by supporting high-speed media and high-density configurations; using the processing capabilities of the Versatile Interface Processors and Cisco Express Forwarding—the Cisco 7500 series system capacity can exceed two million packets per second
- Full support for Cisco IOS software and enhancements for high-performance network services—Performs network services such as quality of service, security, compression, and encryption at high speed; VIP technology extends the performance of these services through distributed IP services
- High port density—Provides high port density and an extensive range of LAN and WAN media; this feature dramatically reduces the cost per port and allows a flexible configuration
- Unmatched interface flexibility—The Cisco 7500 supports a broad selection of Interface Processors (IPs) and Port Adapters (PAs). Port adapters are shared with the Cisco 7200, 7400, and 7600 (with FlexWAN Module)
- High Availability—Enhanced features and capabilities include redundant route processors, power supplies, fans, and software fault isolation with Stateful Switchover and NonStop Forwarding

Competitive Products

• Redback: SMS-500, SMS-1800	• Unisphere: ERX700, ERX1400
• Juniper: M5, M10, M20	• Huawei: NE8 and NE16

Specifications

Feature	Cisco 7505	Cisco 7507	Cisco 7513
Fixed Ports	None	Same as Cisco 7505	Same as Cisco 7505
Expansion Slots	5	7	13
WAN Interface Range	DS0 to OC-12	Same as Cisco 7505	Same as Cisco 7505
Processor	MIPS RISC Processor	Same as Cisco 7505	Same as Cisco 7505
Forwarding Rate	Up to 1.1 Mpps	Up to 2.2 Mpps	Up to 2.2 Mpps
Backplane Capacity	1 Gbps	2 Gbps	2 Gbps
Flash PCMCIA Memory	16MB (expandable to 128MB)	Same as Cisco 7505	Same as Cisco 7505
System DRAM Memory	32MB (expandable to 1GB)	Same as Cisco 7505	Same as Cisco 7505
Minimum Cisco IOS Release	11.3	Same as Cisco 7505	Same as Cisco 7505
Internal Power Supply	AC or DC	AC, dual AC/DC, or dual DC	AC, dual AC/DC, or dual DC
Redundant Power Supply Support	No	Yes	Yes
Chassis Size	6 RU	13 RU	20 RU
Rack Mountable	Yes, up to 6 per rack	Yes, up to 3 per rack	Yes, up to 2 per rack
Dimensions (HxWxD)	10.5 x 17.5 x 17 in.	19.25 x 17.5 x 25 in.	33.75 x 17.5 x 22 in.

Selected Part Numbers and Ordering Information[1]

Cisco 7500 Series Products	
CISCO7505/4	Cisco 7505 5-Slot, 1 CyBus, 1RSP4, Single Power Supply
CISCO7507/8-MX	Cisco 7507, 7 Slot, MIX-Enabled, Dual Bus, 1 RSP8, 1 PS
CISCO7507/8X2-MX	Cisco 7507, 7 Slot, MIX-Enabled, Dual Bus, 2 RSP8, 2 PS
CISCO7507/4	Cisco 7507 7-Slot, 2 CyBus, 1RSP4, Single Power Supply
CISCO7507/4X2	Cisco 7507 7-Slot, 2 CyBus, 2 RSP4, Dual Power Supply
CISCO7513/4	Cisco 7513 13-Slot, Dual Bus, 1RSP4, 1 PS
CISCO7513/4X2	Cisco 7513 13-Slot, Dual Bus, 2 RSP4, 2 PS
CISCO7513/8-MX	Cisco 7513, 13 Slot, MIX-Enabled, Dual Bus, 1 RSP8, 1 PS
CISCO7513/8X2-MX	Cisco 7513, 13 Slot, MIX-Enabled, DualBus, 2 RSP8, 2 PS
CISCO7507/16-MX	Cisco 7507, 7 Slot, MIX-Enabled, Dual Bus, 1 RSP16, 1 PS
CISCO7507/16X2-MX	Cisco 7507, 7 Slot, MIX-Enabled, Dual Bus, 2 RSP16, 2 PS
CISCO7513/16-MX	Cisco 7513, 13 Slot, MIX-Enabled, DualBus, 1 RSP16, 1 PS
CISCO7513/16X2-MX	Cisco 7513, 13 Slot, MIX-Enabled, Dual Bus, 2 RSP16, 2 PS
Cisco 7500 Series Processors and Accessories	
RSP2=	CISCO 7507/7513 ROUTE SWITCH PROCESSOR SPARE
RSP2/2	DUAL RSP2 OPTION FOR 7507 and 7513
CAB-RSP2CON=	RSP2 Console Cable (Spare)
CAB-RSP2AUX=	RSP2 Auxiliary Cable (Spare)
RSP4+=	Cisco 7500 Series Route Switch Processor 4+ (Spare)
RSP8=	Cisco 7505/7507/7513/7576 Route Switch Processor (Spare)
RSP16=	CISCO 7500 ROUTE SWITCH PROCESSOR 16 Spare
Route Switch Processor Memory Options (RSP1 & RSP2)	
MEM-RSP-FLC8M=	RSP Flash Credit Card: 8 MB Kit
MEM-RSP-FLC16M=	RSP Flash Credit Card: 16 MB Kit
MEM-RSP-FLC20M=	RSP Flash Credit Card: 20 MB Kit
MEM-RSP-FLC32M=	RSP2 Flash Card: 32MB Kit
MEM-RSP-16M=	RSP 16 MB DRAM Upgrade Kit
MEM-RSP-32M=	RSP 32MB DRAM Upgrade Kit
MEM-RSP-64M=	RSP 64MB DRAM Upgrade Kit
MEM-RSP-128M=	RSP 128MB DRAM Upgrade Kit
Route Switch Processor Memory Options (RSP4)	
MEM-RSP4-FLC16M=	RSP4 Flash Card: 16 MB Kit
MEM-RSP4-FLC20M=	RSP4 Flash Card: 20 MB Kit
MEM-RSP4-FLC32M=	RSP4/4+ Flash Card: 32 MB Kit
MEM-RSP4-32M=	RSP4 32MB DRAM Upgrade Kit
MEM-RSP4-64M=	RSP4/RSP4+ 64MB DRAM Upgrade Kit
MEM-RSP4-128M=	RSP4/RSP4+ 128MB DRAM Upgrade Kit
MEM-RSP4-128-4PK=	RSP4 128MB DRAM Upgrade Kit (4-pack)
MEM-RSP4-256M=	RSP4/RSP4+ 256MB DRAM Upgrade Kit
MEM-RSP4-256-4PK=	RSP4 256MB DRAM Upgrade Kit (4-pack)
MEM-16F-RSP4+=	RSP4+ 16MB Boot Flash (Spare)
MEM-V250-128-10PK=	128 MByte DRAM Upgrade for VIP2-50/xIP-50 (10-pack)
Route Switch Processor Memory Options (RSP8)	
MEM-RSP8-64M=	RSP8 64MB DRAM Option
MEM-RSP8-128M=	RSP8 128MB DRAM Upgrade Kit
MEM-RSP8-256M=	RSP8 256MB DRAM Upgrade Kit
MEM-RSP8-FLC16M=	RSP8 Flash Card: 16 MB Kit
MEM-RSP8-FLC20M=	RSP8 Flash Card: 20 MB Kit
MEM-RSP8-FLC32M=	RSP8 Flash Card: 32 MB Kit
MEM-RSP8-FLD48M=	RSP8 Flash Oisk: 48 MB Kit
MEM-RSP8-FLD128M=	RSP8 Flash Disk: 128 MB Kit
Route Switch Processor Memory Options (RSP16)	
MEM-RSP16-FLO48M=	RSP16 Flash Disk: 48 MB Option
MEM-RSP16-FLD128M=	RSP16 Flash Disk: 128 MB Option
MEM-RSP16-128M=	RSP16 128MB ECC SDRAM Memory Spare
MEM-RSP16-256M=	RSP16 256MB ECC SDRAM Memory Spare
MEM-RSP16-512M=	RSP16 512MB ECC SDRAM Memory Spare
MEM-RSP16-1G=	RSP16 1GB ECC SDRAM Memory Spare
CISCO7500 Series Gigabit Ethernet Interface Processor	
GEIP=	Gigabit Ethernet Interface Processor
GEIP+=	Enhanced Gigabit Ethernet

Cisco 7500 Series Interface Processors	
CX-CIP2-ECA1=	CHANNEL IP:CIP2 W/ ECA-1 PORT
CX-CIP2-ECA2=	CHANNEL IP:CIP2 W/ ECA-2 PORTS
FEIP2-DSW-2TX=	2-Port Fast Ethernet IP with Dist. Switching (100TX)
FEIP2-DSW-2FX=	2-Port Fast Ethernet IP with Dist. Switching (100FX)
CX-ECA1-U	ESCON Interface Upgrade for CX-CIP-ECA1 or CX-CIP-PCA1
Cisco 7500 Series Versatile Interface Processors	
VIP2-40=	VERSATILE INT. PROCESSOR-2,MODEL 40
VIP2-50=	Versatile Interface Processor 2, Model 50
VIP2-10/15-UPG	VIP2-10 to VIP2-15 Upgrade
VIP2-10/40-UPG	VIP2-10 TO VIP2-40 UPGRADE
VIP2-15/40-UPG	VIP2-15 to VIP2-40 Upgrade
VIP2-20/40-UPG	VIP2-20 TO VIP2-40 UPGRADE
VIP4-50=	Versatile Interface Processor 4, Model 50
VIP4-80=	Versatile Interface Processor 4, Model 80
VIP6-80=	Services Accelerator Versatile Interface Processor 6-80
Cisco 7500 Series Transceiver Modules	
GBIC-SX=	Gigabit Intf. ConverterFor 1000BASE-SX (Short Wavelength)
GBIC-LX/LH=	Gigabit Interface Converterfor 1000BASE-LX standard
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX
POM-OC3-MM	1-port OC3/STM1 Pluggable Optic Module,MM
POM-OC3-SMIR	1-port OC3/STM1 Pluggable Optic Module, SM-IR
POM-OC3-SMLR	1-port OC3/STM1 Pluggable Optic Module, SM-LR
Cisco 7500 VIP2 Memory Options	
MEM-VIP240-32M	32 MB DRAM Option for VIP2-40 (Default)
MEM-VIP240-64M=	64 MB DRAM Option for VIP2-40 (Spare)
MEM-V240-64-10PK=	64 MByte DRAM Upgrade for VIP2-40 (10-pack)
MEM-V250-128-10PK=	128 MByte DRAM Upgrade for VIP2-50/xIP-50 (10-pack)
MEM-VIP250-32M-D=	32 Mbytes DRAM Option for VIP2-50/xIP-50 (default)
MEM-VIP250-64M-D=	64 Mbytes DRAM Option for VIP2-50/xIP-50
MEM-VIP250-128M-D=	128 Mbytes DRAM Option for VIP2-50/xIP-50
MEM-VIP250-4M-S=	4 Mbytes SRAM Option for VIP2-50/xIP-50 (default)
MEM-VIP250-8M-S=	8 Mbytes SRAM Option for VIP2-50/xIP-50
Cisco 7500 VIP4 Memory Options	
MEM-VIP4-64M-SD=	64 MB SDRAM Option for VIP4 (Spare)
MEM-VIP4-128M-SD=	128 MB SDRAM Option for VIP4
MEM-VIP4-256M-SD=	256 MB SDRAM Option for VIP4
Cisco 7500 VIP6 Memory Options	
MEM-VIP6-64M-SD=	64 MB SDRAM Option for VIP6 (Spare)
MEM-VIP6-128M-SD=	128 MB SDRAM Option for VIP6
MEM-VIP6-256M-SD=	256 MB SDRAM Option for VIP6
Cisco 7500 Series Memory Upgrades	
VIP2-10/15/FE2-UPG	DRAM MEM Upgrade for VIP2-10, VIP2-15, CX-FEIP2-2TX AND -2FX
V2-10/15/FE2-UPG=	DRAM MEM Upgrade for VIP2-10, VIP2-15, CX-FEIP2-2TX AND -2FX
Cisco 7500 Series Port Adapters	
PA-A3-OC12SMI=	1 Port ATM Enhanced OC12/STM4 single mode intermediate reach
PA-A3-OC12MM=	1 Port ATM Enhanced OC12/STM4 multi-mode
PA-A1-OC3SM	1 Port ATM OC3 Single Mode Intermediate Reach Port Adapter
PA-A1-OC3MM=	1-Port ATM OC3 Multimode Port Adapter
GEIP+=	Enhanced Gigabit Ethernet
Cisco7200, 7400 and 7500 Series Port Adapters[2]	
Cisco7400 and 7500 Series Port Adapters[3]	
Cisco 7500 Service Adapters	
SA-ENCRYPT=	Encryption Service Adapter - Spare

Cisco 7500 Series CIP Options and Accessories

MEM-CIP-8M=	8 MB Memory, Replaces Existing CIP Memory, Total 8 MB
MEM-CIP-32M=	CIP 32 MB DRAM Upgrade Kit
MEM-CIP-64M=	CIP 64 MB DRAM Upgrade Kit
MEM-CIP-128M=	CIP 128 MB DRAM Upgrade Kit
FR-CIP-CSNA=	SNA SUPPORT FEATURE FOR CIP
FR-CIP-TCPOFF=	TCP/IP OFFLOAD FEATURE FOR CIP
FR-CIP-TN3270S-L=	TN3270 Server - Limited 2000 Session Support
FR-CIP-TN3270S-LS=	TN3270 Server - Limited 2000 Session Support SSL
FR-CIP-TN3270S-MS=	TN3270 Server - Mid-tier 5000 Session Support SSL
FR-CIP-TN3270S-US=	TN3270 Server - Unlimited CIP2 Support SSL
FR-CIP-TNUPG-L-S=	TN3270 Server Upgrade 2,000 Sessions To SSL
FR-CIP-TNUPG-M-S=	TN3270 Server Upgrade 5,000 Sessions To SSL
FR-CIP-TNUPG-U-S=	TN3270 Server Upgrade Unlimited Sessions To SSL
FR-CIP-TNUPG-LM-S=	TN3270 Server Upgrade From 2,000 Sessions To 5,000 SSL
FR-CIP-TNUPG-MU-S=	TN3270 Server Upgrade From 5,000 Sessions To Unlimited SSL
FR-CIP1-TN3270S-G=	CIP1: TN3270 Server Upgrade, Limited to Unlimited Version
FR-CIP2-TN3270S-G=	CIP2: TN3270 Server Upgrade, Limited to Unlimited Version
FR-CIP2-TN3270S-M=	TN3270 Server - Mid-tier 5000 session support
FR-CIP1-TN3270S-U=	TN3270 Server - Unlimited CIP1 Support
FR-CIP2-TN3270S-U=	TN3270 Server - Unlimited CIP2 Support
FR-CIP1-TNUPG-G-S=	TN3270 Server upgrade, limited to unlimited version with SSL
FR-CIP2-TNUPG-G-S=	CIP2: TN3270 Server upgrade, limited to unlimited -SSL
FR-CIP2-TNUPG-LM=	TN3270 server upgrade from 2000 to 5000 sessions
FR-CIP2-TNUPG-MU=	TN3270 server upgrade from 5000 to unlimited sessions
FR-CIP-SNASWITCH=	TN3270 Server - SNA Session Switch Feature
FR-CIP-ASSIST	TCP Assist Feature on CIP for host using Cisco IOS for S/390

NetFlow Utility Software

NDA-HPUX-3.X-UPG	Upgrade To Analyzer 3.6 For HP U/X Incl NFC 35
NDA-SOSU-3.X-UPE	Upgrade To Analyzer 3.6 For Solaris Incl NFC 3.5
NDA-HPUX-3.X-UPE	Upgrade To Analyzer 3.6 For HP U/X Incl NFC 35

Cisco 7500 RSP Feature Licenses

FR-WPP75=	Cisco IOS RSPx Series WAN Packet Protocols/Netflow License
FR-IR75=	Cisco IOS RSP Series InterDomain Routing License
FR75-AN2=	Cisco IOS 7500 Series DBConn

Cisco 7500 Series IOS Feature Licenses

FR75-APPN=	Cisco IOS RSPx Series APPN Upgrade
FR75-BS-A=	Cisco IOS RSPx Series Desktop/IBM to Enterpise
FR75-C-DS=	Cisco IOS RSPx Series IP to IP/IPX/IBM
FR75-C-BS=	Cisco IOS RSPx Series IP to Desktop/IBM
FR75-C-A=	Cisco IOS RSPx Series IP to Enterprise
FR75-DS-BS=	Cisco IOS RSPx IP/IPX/IBM to Desktop/IBM
FR75-DS-A=	Cisco IOS RSPx IP/IPX/IBM to Enterprise
FR75-40=	Cisco IOS RSPx Encryption 40 Upgrade
FR75-56=	Cisco IOS RSPx Encryption 56 Upgrade
FL75-H=	Cisco IOS 7500 Series Firewall/IDS Upgrade
FL75-K2=	Cisco IOS 7500 Series IPSEC 3DES Upgrade
FL75-L=	Cisco IOS 7500 Series IPSEC 56 Upgrade
FL75-R1=	Cisco IOS RSPx Series SNASwitch Upgrade
FL75-N-R1=	Cisco IOS 7500 Series APPN to SNASwitch Upgrade
FR-ITP-HSL=	IP Transfer Point (ITP) High Speed Link (HSL) License

Cisco 7500 Series IOS Feature Set Upgrades

FR-ITP-M3UA/SUA=	IP Transfer Point M3UA/SUA Functionality License
FR-ITP-M2PA=	IP Transfer Point M2PA Functionality Feature License

Versatile Interface Processor Port Adapters (VIP2 and VIP4)

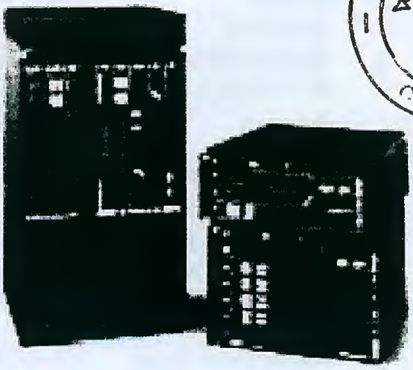
PA-MC-8TE1+=	8 port multichannel T1/E1 8PRI port adapter

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.
2. Cisco 7200, 7400 and 7500 share many port adapters. Please see Cisco 7200, 7400 and 7500 Series Port Adapters, page 1-34 for additional part numbers.
3. Cisco 7400 and 7500 share many port adapters. Please see Cisco7400 and 7500 SeriesPort Adapters, page 1-43 for additional part numbers.

For More Information

See the Cisco 7500 Series Web site: **http://www.cisco.com/go/7500**

Cisco 7600 Series



The Cisco 7600 Series combines optical WAN/MAN networking and high-volume Ethernet aggregation with a focus on line-rate delivery of high-touch IP services in large data centers and at the edge of service provider networks. It provides customers the flexibility of three different form factors: Cisco 7603, 7606, and 7609. As the most scalable system in the industry, each router offers the ability to deliver DS0 to OC-48 WAN connectivity, and 10-Mbps Ethernet to 10-Gigabit Ethernet LAN connectivity into Internet data center, metropolitan aggregation, WAN edge aggregation, and enterprise networking applications.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7603	• 3 slot (horizontal) chassis • 32 Gbps backplane bandwidth • 15 Mpps forwarding rate • NEBs Compliant
Cisco 7606	• 6 slot (horizontal) chassis • 160 Gbps backplane bandwidth • 30 Mpps forwarding rate • NEBs Compliant
Cisco 7609	• 9 slot (vertical) chassis • 256 Gbps backplane bandwidth • 30 Mpps forwarding rate • NEBs Compliant

Key Features

- Hardware accelerated IP services on each Optical Services Module (OSM), delivering up to 6 Mpps per slot
- 15 to 30 Mpps forwarding processor and up to 512 MB DRAM for Internet routing
- Modular and scalable from 32 Gbps to 256 Gbps switch fabric
- One of the widest, most complete ranges of WAN interfaces in the industry, with DS0 to OC-48 connectivity
- Leveraging the FlexWAN Module, 7x00 port adapters are shared with the Cisco 7200, 7300, 7400, and 7500 which simplifies sparing and protects customer investment in interfaces
- Compatible with Catalyst 6500 LAN interfaces, offering 10 Mbps Ethernet to 1 Gbps

Competitive Products

- Redback: SMS-500, SMS-1800
- Juniper: M5, M10, M20, M40
- Unisphere: ERX700, ERX1400
- Extreme: Black Diamond 6808

Specifications

Feature	Cisco 7603	Cisco 7606	Cisco 7609
Fixed Ports	None	Same as Cisco 7603	Same as Cisco 7603
Expansion Slots	3 (horizontal)	6 (horizontal)	9 (vertical)
WAN Interface Range	DS0 to OC-48	Same as Cisco 7603	Same as Cisco 7603
Processor	Supervisor Engine 2 w/MSFC2 and PFC2	Same as Cisco 7603	Same as Cisco7603
Forwarding Rate	Up to 15 Mpps	Up to 30 Mpps	Up to 30 Mpps
Backplane Capacity	32 Gbps	160 Gbps	256 Gbps
Flash PCMCIA Memory	16MB (expandable to 24MB)	Same as Cisco 7603	Same as Cisco 7603
System DRAM Memory	128MB (expandable to512MB)	Same as Cisco 7603	Same as Cisco 7603
Minimum Cisco IOS Release	12.1(8)AE3	Same as Cisco 7603	12.1(8)(A)EX
Internal Power Supply	AC or DC (1000 W)	AC or DC (1000 W)	AC or DC (1300 or 2500 W)
Redundant Power Supply Support	Yes	Same as Cisco 7603	Same as Cisco 7603
Chassis Height	4 RU	7 RU	20 RU
Rack Mountable	Yes, up to 10 per rack	Yes, up to 6 per rack	Yes, up to 2 per rack
Dimensions (HxWxD)	7 x 17.37 x 21.75 in.	12.25 x 17.37 x 21.75 in.	25.2 x 17.2 x 18.1 in.

Selected Part Numbers and Ordering Information[1]

Cisco 7609 Systems	
CISCO7609	7609 Chassis Bundles
7609-AC-BUN	Enhanced 7609 Chassis, SUP2/MSFC2, 4000W AC P/S, 512MB DRAM
7609-DC-BUN-2500W	Enhanced 7609 Chassis, SUP2/MSFC2, 2500W DC P/S, 512MB DRAM
OSR-7609-AC	7609 Chassis, SUP2/MSFC2, 2500W AC P/S, 512MB DRAM
OSR-7609-DC	7609 Chassis, SUP2/MSFC2, 2500W DC P/S, 512MB DRAM
Cisco 7606 Systems	
CISCO7606	Cisco 7606 Chassis Bundle
7606-AC-BUN	7606 Chassis, SUP2/MSFC2, 1900W AC P/S, PEM, 256MB DRAM
7606-DC-BUN	7606 Chassis, SUP2/MSFC2, 1900W DC P/S, PEM, 256MB DRAM
CISCO7606-CHASS	Cisco 7606 Chassis
Cisco 7603 Systems	
CISCO7603	Cisco 7603 Chassis Bundle
7603-AC-BUN	7603 Chassis, SUP2/MSFC2, 950W AC P/S, PEM, 256MB DRAM
7603-DC-BUN	7603 Chassis, SUP2/MSFC2, 950W DC P/S, PEM, 256MB DRAM
CISCO7603-CHASS	CISCO 7603 Chassis
Cisco 7600 Optical Services Modules (OSMs)	
OSM-1CHOC12/T1-SI=	1-port CHOC-12/CHSTM-4 OSM IR, to DS0 and T1/E1, w/4GE
OSM-12CT3/T1=	12-port Channelized DS-3 to DS-1/DS-0
OSM-1CHOC48/T3-SS=	1-port CHOC-48/CHSTM-16 OSM, to T3/E3, SM-SR, with 4 GE
OSM-1CHOC12/T3-SI=	1-port CHOC-12/CHSTM-4 OSM, to T3/E3, SM-IR, with 4 GE
OSM-1OC48-POS-SI=	1-port OC-48/STM-16 SONET/SDH OSM, SM-IR, with 4 GE
OSM-1OC48-POS-SL=	1-port OC-48/STM-16 SONET/SDH OSM, SM-LR, with 4 GE
OSM-1OC48-POS-SS=	1-port OC-48/STM-16 SONET/SDH OSM, SM-SR, with 4 GE
OSM-2OC12-ATM-MM=	2-port OC-12/STM-4 ATM OSM, MM, with 4 GE
OSM-2OC12-ATM-SI=	2-port OC-12/STM-4 ATM OSM, SM-IR, with 4 GE
OSM-2OC12-POS-MM=	2-port OC-12/STM-4 SONET/SDH OSM, MM, with 4 GE
OSM-2OC12-PDS-SI=	2-port OC-12/STM-4 SONET/SDH OSM, SM-IR, with 4 GE
OSM-2OC12-POS-SL=	2-port OC-12/STM-4 SONET/SDH OSM, SM-LR, with 4 GE
OSM-4GE-WAN-GBIC=	4-port Gigabit EthernetOptical Services Module, GBIC
OSM-4OC3-POS-SI=	4-port OC-3/STM-1 SONET/SDH OSM, with 4 GE
OSM-4OC12-POS-MM=	4-port OC-12/STM-4 SONET/SDH OSM, MM, with 4 GE
OSM-4OC12-POS-SI=	4-port OC-12/STM-4 SONET/SDH OSM, SM-IR, with 4 GE
OSM-4OC12-POS-SL=	4-port OC-12/STM-4 SONET/SDH OSM, SM-LR, with 4 GE
OSM-8OC3-POS-MM=	8-port OC-3/STM-1 SONET/SDH OSM, MM, with 4 GE
OSM-8OC3-POS-SI=	8-port OC-3/STM-1 SONET/SDH OSM, SM-IR, with 4GE
OSM-8OC3-POS-SL=	8-port OC-3/STM-1 SONET/SDH OSM, SM-LR, with 4 GE
OSM-16OC3-POS-MM=	16-port OC-3/STM-1 SONET/SDH OSM, MM, with 4 GE
OSM-16OC3-POS-SI=	16-port OC-3/STM-1 SONET/SDH OSM, SM-IR, with 4 GE
OSM-16OC3-POS-SL=	16-port OC-3/STM-1 SONET/SDH OSM, SM-LR, with 4 GE
OSM-2OC48/1DPT-SS=	2-port OC-48/STM-16 POS/DPT OSM, SM-SR, with 4 GE
OSM-2OC48/1DPT-SI	2-port OC-48/STM-16 POS/DPT OSM, SM-IR, with 4 GE

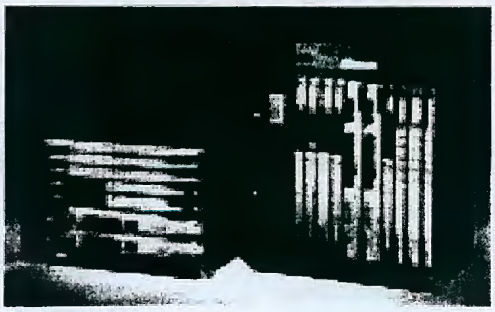
OSM-2OC48/1OPT-SL=	2-port OC-48/STM-16 POS/DPT OSM, SM-LR, with 4 GE
Cisco 7600 Line Cards	
WS-F6K-DFC=	Distributed Forwarding Card
WS-X6348-RJ-45=	Catalyst 6000 48-port 10/100, Upgradable to Voice, RJ-45
WS-X6516-GBIC=	Catalyst 6500 16-port GigE Mod: fabric-enabled (Req. GBICs)
WS-X6524-100FX-MM=	Catalyst 6500 24-port 100FX, MT-RJ, fabric-enabled
WS-X6502-10GE=	Catalyst 6500 10 Gigabit Ethernet Base Module(Req OIM),Spare
WS-X6816-GBIC=	Catalyst 6500 16-port GigE mod, 2 fab I/F w/DF, (Req GBICs)
WS-X6548-RJ-21=	Catalyst 6500 48-port 10/100, RJ-21, fabric-enabled
WS-X6548-RJ-45=	Catalyst 6500 48-port 10/100, RJ-45, x-bar
WS-X6516-GE-TX=	Catalyst 6500 16-port Gig/Copper Module, x-bar
Cisco 7600 Memory Options	
MEM-OSM-64M=	64MB ECC Memory for Optical Services Modules
MEM-OSM-128M	128 MB ECC Memory for Optical Services Modules
MEM-OSM-256M	256 MB ECC Memory for Optical Services Modules
MEM-OSM-512M	512 MB ECC Memory for Optical Services Modules

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 7600 Series Web site: **http://www.cisco.com/go/7600**

Cisco 10000 Series



The Cisco 10000 Series is the industry's only edge router that delivers consistent, high performance services for carriers deploying IP, MPLS, and broadband services to DSL and private line customers. Coupled with proven high availability and innovative adaptive network processing technology, the Cisco 10000 Series is uniquely designed to meet the service needs of carriers up to DS3/E3 aggregation speeds.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 10008	• Broadband features including PPP over ATM, PPP over Ethernet, routed bridge encapsulation, and Layer 2 Tunneling Protocol • MPLS, MPLS VPN, and MPLS Quality of Service edge features • Leased line features such as seamless integration from a dedicated access environment (TDM or SONET/SDH) to the ATM core.

Key Features

- Industry-leading high availability—nonstop performance, with a complete set of reliability features for high availability (99.999 percent uptime). Full hardware redundancy, hot-swappable elements, and seamless route processor cutover provide continuous traffic forwarding.
- Lowest total cost of ownership—the Cisco 10000 offers the highest leased-line, ATM, frame, and broadband session densities on a single platform, and its high reliability reduces network downtime and operational expenses
- Broad portfolio of line-rate IP sessions—critical service features, such as QoS, MPLS, Multilink PPP, and ACLs are hardware accelerated to deliver exceptional throughput for every connection

- Industry-leading session density—the Cisco 10000 supports thousands of DS0, DS1/E1 connections, or hundreds of clear-channel DS3 connections on a single platform, providing the highest port density of DS3-and-below interfaces

Competitive Products

- Redback: SMS-10000
- Juniper: M5, M10, M20
- Unisphere: ERX700, ERX1400

Specifications

Feature	Cisco 10008
Fixed Ports	None
Expansion Slots	8 (for interfaces)
WAN Interface Range	DS0 to OC-12
Processor	Cisco PXF Processor
Forwarding Rate	10005Up to approximately6 Mpps
Backplane Capacity	51.2 Gbps
Flash PCMCIA Memory	48 MB (expandable to 128 MB)
System DRAM Memory	512 MB
Minimum Cisco IOS Release	12.0(9)SL
Internal Power Supply	AC or DC, dual option
Redundant Power Supply	Yes, for both AC and DC
Chassis Height	13 RU
Rack Mountable	Yes, up to 3 per rack
Dimensions (HxWxD)	21.75 x 17.5 x 12 in.

Selected Part Numbers and Ordering Information[1]

Cisco 10008 Pricing Bundles	
ESR10008-1P1AC	C10000 8-slot chassis,1 PRE, 1 AC PEM
ESR10008-1P1AC+6	C10000 8-slot chassis,1 PRE, 1 AC PEM,1CT3 module
ESR10008-1P1DC	C10000 8-slot chassis,1 PRE, 1 DC PEM
ESR10008-1P1DC+6	C10000 8-slot chassis,1 PRE, 1 DC PEM,1CT3 module
ESR10008-1P1AC+4CH	C10000 8-slot chassis, 1 PRE, 1 AC PEM, 1 CH STM-1 Module
ESR10008-1P1DC+4CH	C10000 8-slot chassis, 1 PRE, 1 DC PEM, 1 CH STM-1 Module
ESR10008-2P2AC	C10000 8-slot chassis,2 PREs, 2 AC PEMs
ESR10008-2P2AC+6	C10000 8-slot chassis,2 PREs, 2 AC PEMs,1 CT3 module
ESR10008-2P2DC	C10000 8-slot chassis,2 PREs, 2 DC PEMs
ESR10008-2P2DC+6	C10000 8-slot chassis,2 PREs, 2 DC PEMs,1 CT3 module
ESR10008-2P2AC+4CH	C10000 8-slot chassis, 2 PREs, 2 AC PEMs, 1 CH STM-1 Module
ESR10008-2P2DC+4CH	C10000 8-slot chassis, 2 PREs, 2 DC PEMs, 1 CH STM-1 Module
ESR10008-1P1DC-SK	ESR10008 BBA Starter Kit with PRE1, DC, 4-port OC3, GE
Cisco 10005 Pricing Bundles	
ESR10005-1P1AC	C10000 5-slot chassis, 1 PRE, 1 AC PEM
ESR10005-1P1DC	C10000 5-slot chassis, 1 PRE, 1 DC PEM
ESR10005-1P1AC+6	C10000 5-slot chassis, 1 PRE, 1 AC PEM, 1 CT3 Module
ESR10005-1P1DC+6	C10000 5-slot chassis, 1 PRE, 1 DC PEM, 1CT3 Module
ESR10005-1P1AC+4CH	C10000 5-slot chassis, 1 PRE, 1 AC PEM, 1 CH STM-1 Module
ESR10005-1P1DC+4CH	C10000 5-slot chassis, 1 PRE, 1 DC PEM, 1 CH STM-1 Module
ESR10005-2P2AC	C10000 5-slot chassis, 2 PREs, 2 AC PEMs
ESR10005-2P2DC	C10000 5-slot chassis, 2 PREs, 2 DC PEMs
ESR10005-2P2AC+6	C10000 5-slot chassis, 2 PREs, 2 AC PEMs, 1CT3 Module
ESR10005-2P2DC+6	C10000 5-slot chassis, 2 PREs, 2 DC PEMs, 1CT3 Module
ESR10005-2P2AC+4CH	C10000 5-slot chassis, 2 PREs, 2 AC PEMs, 1 CH STM-1 Module
ESR10005-2P2DC+4CH	C10000 5-slot chassis, 2 PREs, 2 DC PEMs, 1 CH STM-1 Module
ESR10005-CHAS=	C10000 5-SLOT CHASSIS, INCL. 5xDS3 EXT CRD,ALM CRD,BWR,SPARE
ESR-PRE1	Performance Routing Engine, 512 DRAM and 32M Flash

Selected Part Numbers and Ordering Information[1]

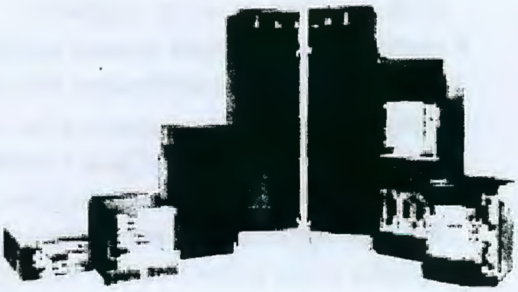
Cisco 10700 Series	
CISCO10720-AC-A	Cisco 10720 Intemet Router with dual AC power supply
CISCO10720-DC-A	Cisco 10720 Internet Router with dual DC Power Supply
10720-FE-TX	24-port 10/100 Ethemet Access Module—RJ45 connectors
10720-FE-FX-MM	24-port 100Mbps Multimode Fiber Ethernet Access Module 2km—MTRJ connectors
10720-FE-FX-SM	24-port 100Mbps Single mode Fiber Ethemet Access Module 15km—MTRJ connectors
10720-GE-FE-TX	4-port 100Mbps SFP GE with 8-ports of 10/100 Ethemet TX-RJ45
10720-SR-LC	OC-48c/STM-16c SRP Short Reach (2km) Uplink Module—LC connectors
10720-IR-LC	OC-48c/STM-16c SRP Intermediate Reach (15km) Uplink Module—LC connectors
10720-LR1-LC	OC-48c/STM-16c SRP Long Reach 1 (40km) Uplink Module — LC
10720-LR2-LC	OC-48c/STM-16c SRP Long Reach 2 (80km) Uplink Module-LC connectors
10720-CON-AUX	Console and Auxiliary port that fits in the Upper Slot
10720-SR-LC-POS	OC-48c/STM-16c POS Short Reach (2km) Uplink Module-LC connectors
10720-IR-LC-POS	OC-48c/STM-16c POS Intermediate Reach (15km) Uplink Module-LC connectors
10720-LR1-LC-POS	OC-48c/STM-16c POS Long Reach 1 (40km) Uplink Module - LC
10720-LR2-LC-POS	OC-48c/STM-16c SRP Long Reach 2 (80km) Uplink Module-LC connectors

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 10720 Internet Router Web site: **http://www.cisco.com/go/10700**

Cisco 12000 Series



The Cisco 12000 Series Internet Router is part of Cisco's family of multimillion packets-per-second (mpps) IP and MPLS routing platforms for building profitable networks in today's communications economy. The Cisco 12000 Series is the premier high-end routing platform for service provider backbone and edge applications, enabling service providers to meet the challenge of building packet networks to satisfy services demand while increasing profitability.

The Cisco 12000 Series offers the only portfolio of 10 Gbps per slot systems and interfaces (including Packet over SONET [POS], Dynamic Packet Transport/Resilient Packet Ring [DPT/RPR], and Gigabit Ethernet [GbE]), delivering 10G economies of scale anywhere in the network. The Cisco 12000 Series provides the highest reliability, the richest set of service enablers, the lowest total cost of ownership, and the only proven investment protection, including systems that can be upgraded in the field to increase switching capacity. This innovative combination of features and capabilities enables service providers to build the most competitive IP and MPLS networks.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 12400 Internet Routers (10G)	• 10 Gbps/slot, from 80 to 320 Gbps of non-blocking switching capacity • Supportfor high-density, high-speedinterfaces: ATM, DPT/RPR, POS, GbE/FE rangingfrom channelized DS3 (to DS1) throughOC-192c/STM-64c • 4 10G platforms to choose from: 12416, 320 Gbps, 16 slots, 40 RU; 12410, 200 Gbps, 10 slots, 20 RU; 12406, 120 Gbps, 6 slots, 10 RU; 12404, 80 Gbps, 4 slots, 5 RU • Support for industry-leading QoS/CoS features ideal for peering, transit, POP consolidation, and IDC bandwidth aggregation as well as latency-sensitive applicationslike voice and video • Support for IP or MPLS forwarding • Support for hundredsof thousandsof routes • Proven carrier- class reliabilityand availability through enhancedfeatures such as Online Insertion and Removal, High Availability (RPR+, NSF and SSO) and APS/MPS
Cisco 12000 Internet Routers (2.5G)	• 2.5 Gbps/slot, from 40 to 80 Gbps switching capacity • Supportfor high-density, high-speedinterfaces: ATM, DPT/RPR, POS, GbE/FE rangingfrom channelized DS3 (to DS1) throughOC-48c/STM-16c • 3 chassis to choose from: 12016, 80 Gbps, 16 slots, 40 RU; 12012, 60 Gbps, 12 slots, 32 RU; 12008, 40 Gbps, 8 slots, 14 RU • The 12016 Internet Router is upgradeableto 320 Gbps via an easy, field-installed switch fabric upgrade kit—no need to pull out existing line cards
Cisco 12000 Manager	• An element management solutionto increase service velocity anddecrease operation costs

Key Features

- Proven investment protection, offering full forward compatibility for all line cards, and the only high-end system with a modular, replaceable switch fabric for field-installed capacity upgrades
- Only fully distributed system architecture scales to the edge, supporting backbone- or edge-optimized line cards in the same chassis
- Only platform that maximizes the value of line-rate edge applications with 10G uplinks. By deploying Cisco 12000 Series IP Services Engine (ISE) line cards in Cisco 12400 Internet Routers, Service Providers benefit from line cards optimized for edge applications, while removing the bandwidth bottleneck with full 10 Gbps uplinks using cost-effective VSR optics or 10 GbE for intra-POP connections.
- The only complete priority packet delivery solution set
- Industry's only complete IP QoS and congestion control implementation that uniquely enables premium real-time services such as VoIP and video. Its distributed architecture and class of service features such as priority based congestion control (WRED) and dedicated low latency queuing (MDRR), along with virtual output queuing (VoQ), eliminate head of line blocking (HOL) and maintain packet sequence integrity under all conditions
- Non-service—impacting online insertion and removal (OIR) of components (including switch fabric cards) and front accessibility reduce downtime and simplify maintenance
- High availability features such as Cisco Non Stop Forwarding (NSF) and Cisco Stateful Switchover (SSO) eliminate single points of failure, help maintain system performance, and prevent service interruption. With these features, packet forwarding remains uninterrupted before, during and after a route processor switchover on the Cisco 12000 Series. Coupled with OIR, the faulty route processor can be replaced without affecting operation
- Designed for NEBS compliance to meet service provider carrier-class requirements

Cisco 10000 Series Memory Options

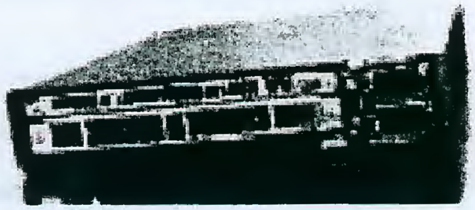
ESR-PRE-MEM-FD48	C10000 PRE 48M Flash Disk (default)
ESR-PRE-MEM-FD128	C10000 PRE 128M Flash Disk option
ESR10005-PWR-AC	AC Power Entry Module
ESR10005-PWR-DC	DC Power Entry Module
ESR-PWR-DC=	DC POWER ENTRY MODULE FOR ESR10008
ESR-PWR-AC	AC power entry module for ESR10008
ESR-PWR-AC/R	Redundant AC powerentry module for ESR10008,spare
ESR10005-PWR-AC=	AC POWER ENTRY MODULE, SPARE
ESR10005-PWR-AC/R	Redundant AC Power Entry Module
ESR10005-PWR-DC/R	Redundant DC Power Entry Module
CAB-DS-ACE	Power Cables for AC Power Option, European
CAB-DS-ACI	Power Cables for AC Power Option, Italian
CAB-DS-ACJ-TWLK	Power Cables for AC Power Option, Japan
CAB-DS-ACU	Power Cables for AC Power Option, UK
CAB-DS-120VAC	Cisco 120 VAC Power Cable,US
ESR-24CT1/E1	24port Channelized E1/T1 Line Card
ESR-8E3/DS3	8 port clear channelE3/DS3 Line Card
ESR-6CT3	6 port channelized T3line card
ESR-1GE	1 pt Gigabit Ethernet line card (requires a GBIC)
ESR-GBIC-SX	1000base-SX GBIC, multimode,standardized forESR
ESR-GBIC-LHLX	1000base-LH GBIC,singlemode,standardizedfor ESR
ESR-GBIC-ZX	1000base-ZX GBIC,singlemode,standardized for ESR
ESR-4OC3ATM-SM	4 Port OC3/STS3c/STM1c ATM Line Card, single mode
ESR-1COC12-SMI	1 pt ChOC12 (STS12) line card, single mode intermed. reach
ESR-1OC12/P-SMI	1 pt OC12/STS12c/STM4 PDS, single mode, int reach
ESR-1OC12ATM-SM	1 pt OC12/STM4 ATM Line Card, Single-Mode

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 10000 Series Web site: **http://www.cisco.com/go/10000**

Cisco 10720 Series



The Cisco 10720 Internet Router is a high-performance router and a principle building block in the metro IP network. It enables service providers to offer innovative and differentiated IP services to their customers at optical speeds. Equipped with Ethernet technology for customer access and the innovative Dynamic Packet Transport (DPT)/RPR (Resilient Packet Ring) technology or Packet over SONET (POS) for metro optical connectivity, the Cisco 10720 allows service providers to offer IP services closer to the user, enabling them to better control admission to network resources. This allows service providers to bypass traditional DS1 and DS3 access options. The dual counter rotating ring technology of DPT is also cost effective, since it uses both rings and can be deployed over dark fiber and still maintain the less than 50ms restoration common in SONET/SDH systems. For multiservice applications, DPT can also be deployed over traditional SONET/SDH ADMs and wavelength division multiplexing (WDM) systems.

The Cisco 10720 is a cost-effective, reliable platform that not only supports the full suite of IP routing protocols such as IS-IS, OSPF and BGP, but also allows advanced IP features to be introduced efficiently, without compromising on performance. Although primarily designed for high-speed Internet services for multitenant and business-park applications in the metro, the Cisco 10720 Internet Router is also suitable for a range of other applications such as: Internet data center applications, intra-POP aggregation, cable multisystem operator (MSO) internetworking, and voice-over-IP (VoIP) aggregation.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 10720 Internet Router	• Any service provider planning to offerhigh-performance IP sevices as part of their business strategy by extending IP further out into the network • Any service provider wanting to simplify their current network and implement thesimple, scalable, reliable features of DPT technology while maximizing fiber usage • Any customer already using DPT technology in their network, most likely with DPT cards on the 12000 Internet Router • Metro Ethernet Servicessuch as L2 and L3 VPN with FE/GE handoff to the Customer and 50ms restoration over dark fiber using DPT.

Key Features

- Equipped with Redundant Power Supply by default
- SRP specific features—IPS with <50 ms restoration time and SRP MIB support
- Multicast support including PIM SM, PIM DM, MBGP
- L2 VPN—UTI, L2TPv3 and EoMPLS for Layer 2 to Layer 2 LAN extension; L3 VPN MPLS VPN
- QoS—Modular QoS CLI, CAR, WRED, VTMS traffic shaping, and access lists
- Ethernet features—MDI-MDI-X support, 10/100 speed auto-negotiation, HDX-FDX negotiation and time delay reflectometry (TDR) for 10/100BaseTX
- Hot Standby Routing Protocol (HSRP)/Multiple Hot Standby Routing Protocol (MHSRP)
- 64-MB built-in Flash for software and configuration load
- Optical receive power monitoring support on OC-48/STM-16 Interface and GE
- Supported management information bases (MIBs) include SNMP, SRP, SONET, Etherlike, OSPF

Competitive Products (vs. Cisco's Metro IP RPR Solution using the 10720)

- Extreme Summit: 48/Blackdiamond comb for GigE Hub & Spoke
- Riverstone: RS3000/RS8600 combo for GigE Hub & Spoke

Specifications

Feature	Cisco 10720
Security Features	Including AAA, RADIUS authentication, TACACS+, and encrypted passwords
Management	Cisco IOS CLI TACACS+ and RADIUS Configuration and administration features including Telnet and CiscoDiscovery Protocol (CDP) Serial (aux) and consoleports for local and remote administration Remote software download via TFTP and RCP IP over DCC for remote management of the Cisco ONS 15104 OC-48/STM-16 Optical Regenerator, where applicable
Physical Interfaces	Uplink Modules: 2-port single-mode OC-48c/STM16c DPT (SR 2 km (1.2 miles), IR 15 km (9.3 miles), LR1 40km (24 miles) and LR2 80km (50miles) Interface Modules—The Cisco 10720 Internet Router has two dedicated slots for interface modules—modulesare not interchangeable or hot swappable: • Upper slot is dedicated for DPT or POS Uplink module equipped withtwo physical ports of OC-48c/STM16c that provide an aggregatebandwidth of approximately 5 Gbps. The cards are available in two four versions of optics, short reach (SR) and intermediatereach (IR), Long Reach1 (LR1) and Long Reach2 (LR2) with two small form-factor OC-48 ports with LC connectors • A third option for the upperslot is the CON-AUX module, which is a depopulated uplinkcard equipped with Console and Auxiliary ports only; this allows the configuration of the 10720 as an "EthernetRouter" allowing the use of one or more of the Ethernet ports in the lower slot for network connectivity • Lower slot is dedicated for24-port Fast Ethernet module—available in TX (100 m reach), FX-MM (2 km reach) or FX-SM (15 km reach). The TX module is equippedwith RJ-45 connectorswhile the FX-SM and FX-MM modules are equipped with MT-RJ connectors. • Also available is a combination 4 Gigabit Ethernetwith Small Form Factor Plug-able(SFP) Optics available in SX 550m and LH 10km plus an additional 8 Ports of Fast Ethernet 10/100 TX Copper ports. The TX and the FX-MM versions of the 24-port Fast Ethernet modules accommodate copper or multimode fiber deploymentswithin MTUs and the FX-SM allows for deployment of the Cisco 10720 Internet Router in a central location covering Ethernet connectivity to buildings for a radius of up to 15 km.
Dimensions	3.5 x 17.25 x 18.25 in. (8.9 x 43.81 x 46.35 cm)

Competitive Products

- Juniper: T640, M160, M40E, M40, and M20
- Avici: Stackable Switch Router (SSR)

Specifications

Feature	Cisco 12008	Cisco 12012	Cisco 12016	Cisco 12404	Cisco 12406	Cisco 12410	Cisco 12416
Switching Capacity	40 Gbps	60 Gbps	80 Gbps	80 Gbps	120 Gbps	200 Gbps	320 Gbps[1]
Capacity per slot (full duplex)	2.5 Gbps	2.5 Gbps	2.5 Gbps	10 Gbps	10 Gbps	10 Gbps	10 Gbps[1]
Chassis Size	1/3 Rack	Full Rack	Full Rack	1/8 Rack	1/4 Rack	1/2 Rack	Full Rack
Chassis Slots	8	12	16	4	6	10	16
Supported Line Cards	All Cisco 12000 Series 2.5 Gbps line cards See Part Numbers and Ordering Information	Same as Cisco 12008	All 2.5 Gbps line cards plus all 10 Gbps line cards when upgraded	Same as Cisco 12416	Same as Cisco 12416	Same as Cisco 12416	All Cisco 12000 Series Line Cards
Supported Protocols	IPv4, MPLS, BGPv4, IS-IS, OSPF v. 2.0, EIGRP, RIP v2, IGMP, PIM (dense and sparse mode)	Same as Cisco 12008	Same as Cisco 12008	Same as Cisco 12416	Same as Cisco 12416	Same as Cisco 12416	IPv4, MPLS, BGPv4, IS-IS, OSPF v. 2.0, EIGRP, RIP v2, IGMP,DVMRP, PIM DM/SM
Management	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager
Dimensions	24.85 x 17.4 x 21.2 in. (63.1 x 44.2 x 53.8 cm)	56 x 17.3 x 21 in. (142.2 x 43.9 x 53.3 cm)	72.5 x 18.75 x 24 in. (184.2 x 47.6 x 61 cm)[2]	8.75 x 18.9 x 27.5 in. (22.23 x 48.01 x 69.85 cm)	18.5 x 18.9 x 28 in. (47 x 48 x 71.1 cm)[3]	37.5 x 19 x 24 in. (95.25 x 48.26 x 61 cm)[4]	72.5 x 18.75 x 24 in. (184,2 x 47.6 x 61 cm)[2]

1. The Cisco 12016 may be field upgraded to a Cisco 12416 via a Switch Fabric Upgrade kit, providing 10 Gbps full duplex capacity per slot, for an overall 320 Gbps switching capacity
2. Includes power, front cover, rack mount flanges, and cable-management system
3. Includes rack-mount flanges, power entry module pullouts, blower, and handle
4. Includes cable-management system and front cover

Selected Part Numbers and Ordering Information[1]

Cisco 12000 Series of Gigabit Switch Routers (GSR)	
GSR6/120-AC	GSR6/120 w/ 1GRP, 3SFC, 1 CSC, 2Alarms & 1 AC Power Supply
GSR6/120-DC	GSR6/120 w/ 1GRP, 3SFC, 1 CSC, 2Alarms & 1 DC Power Supply
GSR8/40	Cisco12008 GSR 40Gbps;1GRP,1CSC-GSR8,3SFC-GSR8,1DC
GSR10/200-AC	Cisco 12410 200 Gbps; 1GRP, 2 CSC, 5 SFC, 2 Alarm, 2 AC
GSR10/200-DC	Cisco 12410 200 Gbps; 1GRP, 2 CSC, 5 SFC, 2 Alarm, 2 DC
GSR12/60	Cisco12012 GSR 60Gbps;1GRP,1CSC,3SFC,1DC
GSR4/80-AC	GSR12404- 4 slot AC System
GSR4/80-DC	GSR12404- 4 slot DC System
GSR16/80-AC-8R	Cisco 12016 80 Gpbs; 1GRP, 2CSC, 3SFC, 2Alarm, 3AC, 8Rails
GSR16/80-AC4-8R	Same As GSR16/80-AC-8R But W/ 4AC And Requires 8 Foot Rack
GSR16/80-DC-8R	Cisco 12016 80 Gpbs; 1GRP, 2CSC, 3SFC, 2Alarm, 4DC, 8Rails
GSR16/320-AC	Cisco 12416 320 Gbps; 1GRP, 2CSC, 3SFC, 2Alarm, 3AC, 8Rails
GSR16/320-AC4	Same As GSR16/320-AC-8R But W/ 4 AC And Requires 8 Foot Rack
GSR16/320-DC	Cisco 12416 320 Gbps; 1GRP, 2CSC, 3SFC, 2Alarm, 4DC, 8Rails
Cisco 12000 Series Processors	
GRP-B	Route Processor, 128MB and 20MB Flash, ECC support
GRP-B/R	GSR Route Processor, Redundant Option
PRP-1	Cisco 12000 Series Performance Route Processor
PRP-1/R	Redundant PRP-1 chassis upgrade option, factory only

Cisco 12000 Series Line Cards

LC-4OC3/POS-SM	4port OC3/STM1 Packet Over SONET/SDH Line Card, Single-Mode
LC-4OC3/POS-MM	4port OC3/STM1 Packet Over SONET/SDH Line Card, Multi-Mode w
LC-1OC12/POS-SM	1port OC12/STM4 Packet Over SONET/SDH Line Card, Single-Mode
LC-1OC12/ATM-MM	1 port OC12/STM4 ATM Line Card, Multi-Mode
LC-1OC12/ATM-SM	1 port OC12/STM4 ATM Line Card, Single-Mode
LC-1OC12/POS-MM	1 port OC12/STM4 Packet Over SONET/SDH Line Card, Multi-Mode
CHOC48/DS3-SR-SC	1 port channelized oC-48 to DS3
2CHØC3/STM1-IR-SC	Channelized OC3/STM1 -> DS1/E1, 2 ports Intermediate Reach
4CHOC12/DS3-I-SCB	4 PORT CHANNELIZED OC12 B
4OC3/ATM-IR-SC	4 port OC3/STM1 ATM Line Card intermediate reach
4OC3/ATM-MM-SC	4 port OC3/STM1 multimode ATM line card
4OC3/POS-LR-SC	4 port OC-3/STM1 SONET/SDH Long Reach LC with SC connector
4OC12/ATM-IR-SC	4 port OC-12/STM4 ATM LC Intermediate Reach
4OC12/ATM-MM-SC	4 port OC-12/STM4 ATM Line Card multimode
4OC12/POS-MM-SC-B	4OC12/POS-MM-SC-B
4OC12X/POS-M-SC-B	4-port OC12/POS Eng3 Multi-mode
4OC12/POS-IR-SC-B	4OC12/POS-IR-SC-B
4OC12X/POS-I-SC-B	4 PORT OC12 PDS B
4OC48/SRP-SFP=	4 Port OC48c/STM16c SRP Linecard, SFP Optics
4OC48E/POS-LR-SC	Edge 4 Port OC-48c/STM-16c SONET/SDH LR with SC
4OC48E/POS-SR-SC	Edge 4 Port OC-48c/STM-16c SONET/SDH SR with SC
8OC03/ATM/TS-IR-B	8-port OC03/STM1 ATM IR LC with SC connector
8OC03/ATM/TS-MM-B	8-port OC03/STM1 ATM MM LC with SC Connector
OC12/SRP-IR-SC-B	OC12 SRP IR line card
OC12/SRP-LR-SC-B	OC12 SRP LR line card
OC12/SRP-MM-SC-B	OC12 SRP MM line card
OC12/SRP-XR-SC	OC12 SRP single ring linecard, single mode 1550, XR
OC48/SRP-LR-SC-B=	DC48 SRP Rev-B Line Card, Single Mode, Long Reach
OC48/SRP-SR-SC-B=	DC48 SRP Rev-B Line Card, Single Mode, Short Reach, GSR
OC48E/POS-LR-SC-B=	1 Port OC-48c/STM-16c SONET/SDH 1550nm LR with SC
DC48E/POS-SR-SC-B=	1 Port OC-48c/STM-16c SONET/SDH 1310nm SR with SC, GSR
OC48X/POS-LR-SC	CONCATENATED OC48 WITH EXTENDED FEATURES LONG REACH
OC48X/POS-SR-SC	1 port OC48 POS Extended features
8OC3/POS-MM=	8 port OC3/STM1 SONET/SDH Multi-Mode LC with MTRJ conn Spare
8OC3/POS-SM=	8 port OC3/STM1 SDNET/SDHSingle-Mode LC with LC conn Spare
1X10GE-LR-SC=	Cisco 12000 1-Port 10GE Card, 1310nm serial, 10km, SC
16OC3/POS-MM=	16 port OC3/STM1 SONET/SDH Multi-Mode LC with MTRJ conn
16OC3/POS-SM=	16 port OC3/STM1 SONET/SDH Single-Mode LC with LC conn Spare
16DC3X/POS-I-LC-B	16 PDRT OC3 WITH EXTENDED FEATURES RELEASE B
EPA-GE/FE-BBRD	Cisco 12000 Modular GE Baseboard w/ 1GE and 3 EPA Slots
EPA-3GE-SX/LH-LC	Cisco 12000 3-Port GE Port Adapter for EPA-GE/FE-BBRD
3GE-GBIC-SC	GSR12000 three-port GE line card
GE-GBIC-SC-B	GSR12000 single port Gigabit Etherret line card
GBIC-SX-MM	1000base-SX GBIC module, multimode,standardized for GSR12000
GBIC-LH-SM	1000base-LH GBIC module,singlemode,standardized for GSR12000
GBIC-ZX-SM	GBIC very long reach GBIC module for the GE line card
6CT3-SMB	Channelized T3for the GSR
GLC-LH-SM	GE SFP, LC connector LHtransceiver
GLC-SX-MM	GE SFP, LC connector SXtransceiver
6DS3-SMB-B	6DS3-SMB-B w/ ECC
6E3-SMB	E3 line card, 6 ports
12DS3-SMB-B	12DS3-SMB-B w/ ECC
12E3-SMB	E3 line card, 12 ports
CHOC12/STS3-IR-SC=	Channelized OC-12/STM-4 with four STS-3c/STM-1 POS paths
LC-OC12-DS3	1 port Channelize OC-12 with 12 DS3s
8FE-FX-SC-B	GSR 8-port 100baseFX, SC connector, version B
8FE-TX-RJ45-B	8-port 100baseTX, RJ45 connectortype, version B
OC192/POS-IR-SC	1 Port OC192c/STM64c POS, 1550nm IR, SC
OC192/POS-SR-SC	1 Port OC192c/STM64c POS, 1310nm SR, SC
OC192/POS-VSR	1 Port OC192c/STM64c POS, VSR Optics
OC192E/POS-VSR	1 Port OC192c/STM64c POS Edge Card, VSR Optics
OC192E/POS-IR-SC	1 Port OC192c/STM64c POS Edge Card, 1550nm IR, SC
OC192E/POS-SR-SC	1 Port OC192c/STM64c POS Edge Card, 1310nm SR, SC
OC192/SRP-VSR	1 Port OC192c/STM64c SRP Linecard, 850nm VSR, MTP
OC192/SRP-IR-SC	1 Port OC192c/STM64c SRP Linecard, 1550nm IR, SC
OC192/SRP-SR-SC	1 Port OC192c/STM64c SRP Linecard, 1310nm SR, SC

4GE-SFP-LC=	4 port-GE line card for Cisco 12000
Cisco 12000 Series Pluggable Optic Modules	
POM-OC48-LR2-LC	1-port OC-48/STM-16 Pluggable Optic Module, 1550nm SM-LR2 LC
POM-OC48-SR-LC	1-port OC-48/STM-16 Pluggable Optic Module, 1310nm SM-SR LC

1. Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 12000 Series Web site: **http://www.cisco.com/go/12000**

Cisco SN 5400 Series Storage Router

The Cisco SN 5400 Series implements the iSCSI protocol to extend access of a Fibre Channel fabric and attached storage devices to IP servers. iSCSI (internet SCSI) combines the benefits of the TCP/IP protocol suite with SCSI, the universal standard for storage access. By utilizing iSCSI, the SN 5400 Series extends a Fibre Channel storage network to lower priced/lower performance servers in a data center and departmental servers located throughout the campus and enterprise. With the SN 5428, access to a Fibre Channel Storage Area Network (SAN) from anywhere on an IP network is as easy as accessing direct attached storage.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco SN 5428	• When a customer is moving from a DAS (Direct Attached Storage) environment to a SAN (Storage Area Network) and they do not already have a Fibre Channel switch, the SN 5428 provides a Fibre Channel switch and iSCSI ports to deliver a one system solution. • When the customer wants only a full function Fibre Channel switch, the SN 5428 is a very cost effective, low latency switch that will perfectly fit a Fibre Channel onlyimplementation • When the customer has block level applications and wants to maintain block level access to shared storage combined with IP/Ethernet for a substantial reduction in attachment costs

Key Features

- Provides levels of security and access control beyond what is currently available in traditional storage area networks by including layer 2 and layer 3 protection to resist against unauthorized access to your storage resources
- Uses the TCP/IP protocol suite for storage networking which protects your existing investment in storage and networking infrastructure
- Fully integrates existing management and configuration tools
- Based on industry standards, maximizes your investment and enables you to reduce total cost of ownership for the increasing storage demands on your network
- Uniquely provides standard IP networking capabilities to storage environments
- SN 5428: Designed for high-availability providing continuous access to critical data; Extensive security features to protect valuable storage resources; and, Full breadth of iSCSI drivers

Competitive Products

- Nishan
- McData: Fibre Channel Switches
- Qlogic: Fibre Channel Switches
- FalconStor
- Brocade: Fibre Channel switches

Selected Part Numbers and Ordering Information[1]

Cisco SN 5428 Storage Router	
SN5428	The SN 5428 provides two Gigabit Ethernetports, supporting iSCSI, for connection to sandard IP networks and eight Fibre Channel fabic switch ports.
Cisco SN 5428 Drivers & Firmware	
SN5428-FW-2.x	Cisco SN 5428 Firmware: 2.2.x minimum (2.2.1 minimum)
SN-ISCSI-DRV=	Cisco iSCSI drivers that support the Cisco SN 5428 2.2.x firmware: Windows NT, Windows 2000, Linux, Solaris, HP/UX, AIX
Cisco SN 5428 SFP: Small Form Factor Pluggables	
SN-SFP-FCMM-LC=	SFP for Fibre Channel Multi-mode fiber with LC connector
SN-SFP-FCMM-LC=	SFP for Fibre Channel Multi-mode fiber with connector spare
SN-SFP-FCGEMM-LC	SFP for GE/FC with LC connector
SN-SFP-FCGEMM-LC=	SFP for GE/FC with LC connector
Cisco SN 5420 Series Packaged SMARTnet Maintenance 8x5xNBD	
CON-SNT-PKG10	Cisco SN 5428 Packaged SMARTnet 8x5xNBD—Category 10

For More Information

See the Cisco SN5420 Series Storage Router Web sites:
http://www.cisco.com/go/sn5428

CHAPTER 2

LAN Switching

LAN Switching Products at a Glance

Product	Features	Page
Catalyst 2900 Series	Fixed-configuration Ethernet switches • 10/100 auto sensing and auto negotiating interface • Managed	2-3
Catalyst 2948G-L3	Fixed and Modularports • Gigabit Ethernet over Fiber or Copper • High performance, CiscoExpress Forwarding (CEF) Layer 2/3/4 switching upto 48 Mpps • Advancednetworkcontrolwith predictable performance,granular QoS,advancedsecurity, comprehensive management	2-3
Catalyst 2900 Series XL—Modular Switches	Modular 10/100 Ethemet switches • 12 or 24 10/100 ports • 12 100BASE- FX ports (2912MF XL) • Two high-speed module slots accommodating 10/100, 100BASE-FX, Gigabit Ethernet (including 1000BASE-T), and GigaStack GBIC (2912MF XL and 2924M XL only) • Cisco switch clustering enabled • Managed	2-4
Catalyst 2950 Series	Fixed-configuration basic and Intelligent Ethernet 10/100 switches • 12/24/48 10/100 port managed switches with stackable andstandalone models • Flexible uplink options: fixed 100Base FX, fixed 1000BaseT, fixed 1000BaseSX, and GBIC-based ports • Industrial-grade, rugged models(Catalyst 2955) for harsh environment deployments • Wire-speed, high performance switch • Models with the Standard Image software (SI)provide Layer 2 Cisco IOS functionality for basic data, voice, and videoservices at the edge of the network • Models with the EnhancedImage software (EI) bring Layer 2-4 intelligentservices such as advanced Qualty of Service, rate limiting, security filteringand multicastmanagement capabilities • Stackable up to 9switcheswith GigastackGBIC • Simplified networkmanagement through Cisco ClusterManagement Suite up to 16fixed configuration Catalyst switches	2-6
Catalyst 3500 Series XL	Fixed-configuration 10/100 and Gigabit Ethernetswitches • 24 ports with 2 GBIC-based Gigabit Ethemet ports with in-line power(3524-PWR XL) • 8 GBIC-based ports (3508G XL) • Stackable up to 9switcheswith GigaStack GBIC • Cisco Switch Clusteringcapable • Managed	2-10
Catalyst 3550 Series	Fixed-configuration IntelligentEthemet switchesin stackable 10/100, inline power, or Gigabit Ethernet configurations • Network controland bandwidth optimization via advanced Quality of Service (QoS), granular rate-limiting, Access ControlLists (ACLs), and multicast services • Network security through a wide range of authentication methods,data encryption technologies,and accessrestrictionfeatures based on users, ports, and MAC addresses • Network scalabilitythroughadvancedrouting protocolssuch as EIGRP, OSPF, BGP, and PIM (requires Enhanced Multilayer Software Image (EMI)) • Intelligent adaptabilitythrough Cisco Identity Based Networking Services (IBNS) offering greater flexibility and mobility to stratified users	2-12

Product	Features	Page
Catalyst 4500 Series-Modular Configuration (4503, 4506 and 4507R)	Modular, multilayer switch with integrated intelligent services for converged networks in enterprise campus wiring closets, Layer2/Layer3 distribution, and integrated LAN/WAN branch office. • Resilient architecture for mission critical applications • Up to 240 ports of Ethernet, Fast Ethernet or Gigabit Ethernet over Fiber or Copper • High performance, CiscoExpress Forwarding (CEF) Layer 2/3/4 switching up to 48 Mpps • Up to 64 Gbps of switching capacity • Advanced network control with predictable performance, granular QoS, advanced security, comprehensive management • Managed	2-15
Catalyst 4000 Series—Fixed Configuration (4908G-L3 and 4912G)	High performance fixed Gigabit Ethernet switch with intelligent enterprise Cisco IOS services	2-17
Catalyst 5000 Family	Modular switch that supports a broad range of interfaces for aggregation of legacy technologies with IP technology • End of Sale Effective June 2003/End of Support effective 2008. For further information please contact your local sales representative	2-18
Catalyst 6500 Family	High-performance, multilayer switch with integrated intelligent services for enterprise campus backbones, server aggregation, or internet data centers • 10/100, 100FX Fast Ethernet, 1000BASE-T, 1000BASE-X, and Gigabit Ethernet modules • Layer 4-7 services • Up to 256 Gbps of switching capacity • Packet throughput scalable to 100+ Mpps • Managed	2-20
Catalyst 8500 Series	High-performance, modular, multimedia switch router • Wire speed, nonblocking IP, IPX, IP multicast Layer 3 switching • Multiple interface options • Managed	2-24

Cisco LAN and MAN Products Port Matrix

	Switches							
	Catalyst 2900	**Catalyst 2900 XL**	**Catalyst 2950**	**Catalyst 3500 XL**	**Catalyst 3550**	**Catalyst 4500**	**Catalyst 6000**	**Catalyst 8500**
Fixed Ports Only	X							
Fixed and Modular Ports		X	X	X	X	X		
Modular Ports Only							X	X
Ports								
10BASE-T Switched	X	X	X	X	X	X	X	
10BASE-FL Switched							X	
100BASE-T Switched	X	X	X	X	X	X	X	
100BASE-F Switched		X	X		X	X	X	X
10/100 Autosensing Switched	X	X	X	X	X	X	X	X
1000BASE-TX							X	
10/100/1000							X	
10GBASE-LR							X	
ATM							X	X
Gigabit Ethernet	X	X	X	X	X	X	X	X
Integrated In-Line Power				X		X	X	
Integrated Server Load Balancing							X	

Cisco Catalyst 2900 Series

The Catalyst 2948G and 2980G deliver all the Ethernet switching needed for many small to medium-sized wiring closets in a single system without the need for additional modules, cables or other interconnects. Utilizing the same industry-leading software and functionality of the Catalyst 4000, 5000, and 6000 families, the Catalyst 2948G and 2980G have consistent end-to-end services, which ensure complete interoperability with enterprise Catalyst switches.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 2980G Series	• A single box solution without additional cables, modules or configuration • Up to 80 ports of wire-speed, non-blocking performance with large MTBF reliability • End-to-end VLANs, EtherChannel, multicasting, and security • Mature/proven Catalyst software compatibility in the wiring closet and data center
Catalyst 2948G Series	• The same features as 2980G but up to 48 ports of wire-speed, non-blocking performance
Catalyst 2948G-L3	• High performance CPU with Cisco IOS software • Dedicated 48 ports of 10/100 Mbps and two ports of 1000BASEX Gigabit Ethernet with gigabit Ethernet converter (GBIC) support; all ports support Layer 3 capability

Key Features

- Powerful non-blocking performance with proven Cisco IOS services
- Wire speed 18 Million pps switching throughput
- Intelligent multilayer IOS services (security, multicast, quality of service [QoS])
- Advanced multiple queue QoS architecture
- Security (TACACS+, RADIUS, port lockdown)
- Spanning-Tree Protocol (802.1D) with enhancements (UplinkFast, PortFast) for deterministic/fast failover
- Redundant Power Supply (option)

Competitive Products

- HP Procurve: 4108gl, 4000M
- 3Com: SS3300
- Nortel/Bay: BayStack 350T and 450T
- Extreme: Summit 48si

Specifications

Feature	Catalyst 2980G	Catalyst 2948G-L3	Catalyst 2948G
Fixed Ports (connections)	80-port 10/100BASE-TX 2-port 1000BASE-X (GBIC)	48 port 10/100BASE-TX 2-port 1000BASE X (GBIC)	48-port 10/100BASE-TX 2-port 1000BASE-X (GBIC)
Backplane	24 Gbps	22 Gbps	24 Gbps
Stackable	No	No	No
Full-Duplex Capabilities	All ports	All ports	All ports
VLAN Maximum	1024	1024	1024
FEC	Yes	No	Yes
ISL	No	Yes	No
802.1Q	Yes	Yes	Yes
Management Capabilities	CiscoWorks 2000, CWSI, CiscoView, CDP, VTP, Enhanced SPAN, SNMP, Telnet Client, BOOTP, TFTP	CiscoWorks 2000, CWSI, CiscoView, CDP, VTP, Enhanced SPAN, SNMP, Telnet Client, BOOTP, TFTP	CiscoWorks 2000, CWSI, CiscoView, CDP, VTP, Enhanced SPAN, SNMP, Telnet Client, BOOTP, TFTP
Processor Speed (Type)	200 MHz (R5000 RISC)	200 MHz (R5000 RISC)	200 MHz (R5000 RISC)
Flash Memory	12 MB	16 MB	12 MB
DRAM Memory	64 MB	64 MB	64 MB

Feature	Catalyst 2980G	Catalyst 2948G-L3	Catalyst 2948G
Embedded RMON	Statistics, history, alarms, events	Statistics,history, alarm, events	Statistics, history, alarms, events
Dimensions (HxWxD)	3.5 x 17.5 x 17 in.	2.69 x 17.1 x 18 in.	2.62 x 17.5 x 15 in.
RPS	Yes (WS-C2980G-A), RPS 300	Yes, RPS 600	Yes, RPS 600

Selected Part Numbers and Ordering Information[1]

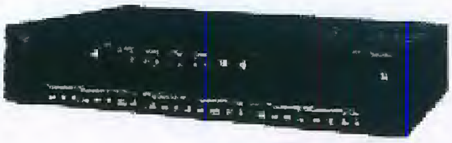
Catalyst 2900 Series Switches	
WS-2948G-L3	Catalyst 2948GL3 Switch
FR2948GL3-IP	Catalyst 2948G-L3 IP Switching License
FR2948GL3-IPX	Catalyst 2948G-L3 IPX Switching License
WS-C2948G	Catalyst 2948G Switch,48 10/100Tx (RJ-45) +2 1000x (GBIC Slots)
WS-C2948G-3PACK	3 Catalyst 2948G Switches
WS-C2980G-A	Catalyst 2980G Switch,80 10/100Tx (RJ-45) +2 1000x (GBIC Slots)
Catalyst 2900 Series Modules	
WS-G5484=	GBIC Module, fiber media SX
WS-G5486=	GBIC Module, fiber media LX/LH
WS-G5487=	GBIC Module, Fiber Media Zx
Mini-RMON Agent License	
WS-C2948G-EMS-LIC	Catalyst 2948G RMON Agent License
WS-C2980G-EMS-LIC	Catalyst 2980G RMON Agent Agreement
Catalyst 2900 Series Accessories	
WS-X2948G-RACK=	Catalyst 2948G Rack Kit (spare)
WS-X2980G-RACK=	Catalyst 2980G Rack Kit (Spare)
PWR600-AC-RPS-CAB=	Redundant Power Supply (RPS), 600 Watts (2948G only)
PWR600-AC-RPS-NCAB=	RPS 600 without Cable (2948G only)
PWR300-AC-RPS-N1=	RPS 300 with one Cable (2980G-A only)
CAB-RPS-1414=	One DC power cable for RPS 300
Catalyst 2900 Series Basic Maintenance	
CON-SNT-PKG8	Catalyst 2948G, 2948G-L3, and 2980G Packaged SMARTnetMaintenance 8x5xNBD

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 2900 Web site: **http://www.cisco.com/go/2900**

Cisco Catalyst 2900 Series XL—Modular Switches



Cisco's Catalyst 2900 Series XL is a full line of modular, 10/100 autosensing Fast Ethernet switches that combine outstanding performance, ease of use, and integrated Cisco IOS software.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 2912MF XL	• All-fiber switch to aggregate Fast Ethernet workgroups over 100BASE-FX connections in small and mid-size campus environments • High-speed uplnks to backbone or server via Fast Ethernet, Gigabit Ethernet
Catalyst 2924M XL	• Any combination of dedicated 10-Mbps or 100-Mbps connections to individual PCs, servers, and other systems or connectivity between existing Ethernet and Fast Ethernet workgroups • The option to easily increase the switch's port density and provide inexpensive high-speed uplinks through bandwidth aggregation (Fast EtherChannel and Gigabit EtherChannel technologies) • Gigabit Ethernet (including 1000BASE-T) modules for high-speed links • Hot swap insertion and removal of modules • Maximum flexibility

Key Features

- Switch fabric of 3.2 Gbps, a forwarding rate of more than 3.0 million packets per second, and a maximum forwarding bandwidth of 1.6 Gbps, delivering wire-speed performance across all 10/100 ports
- Support for IEEE 802.1p protocol for prioritization of mission-critical and time-sensitive applications such as voice and telephony traffic
- Cisco's switch clustering technology enables up to 16 interconnected Catalyst 1900, 2900 XL, and 3500 XL switches, regardless of geographic location, to form a flexible, single IP managed network
- Up to 250 port-based VLANs or ISL/802.1Q trunks
- Network port allows operation in networks with unlimited MAC addresses
- Autoconfiguration of multiple switches on a network from one boot server
- Up to 4 Gbps bandwidth between routers, switches, and servers with Fast EtherChannel and Gigabit EtherChannel technologies

Competitive Products

- 3Com: SuperStack III 3300
- Nortel: BayStack 350 & 450 switches

Specifications

Feature	Catalyst 2912 MF XL	Catalyst 2924M XL
Fixed Ports	12-port 100BASE-FX	24-port 10/100 autosensing
Modular Slots	2	Same as Catalyst 2912MF XL
Available Modules	4-port 10BASE-T/100BASE-TX autosensing 2-port or 4-port switched 100BASE-FX 1-port Gigabit Ethernet(1000BASE-T or GBIC-based)	Same as Catalyst 2912MF XL
Backplane	3.2 Gbps	Same as Catalyst 2912MF XL
Stackable	Yes	Same as Catalyst 2912MF XL
Full Duplex Capabilities	All 10BASE-T, 100BASE-TX, 100BASE-FX, 1000BASE-X, and 1000BASE-T	Same as Catalyst 2912MF XL
VLAN Maximum	250-port-based VLANs or ISL/802.1Q trunks	Same as Catalyst 2912MF XL
FEC	Yes	Same as Catalyst 2912MF XL
Inter-Switched Link	Yes	Same as Catalyst 2912MF XL
Flash Memory	4 MB	Same as Catalyst 2912MF XL
CPU DRAM	8 MB	Same as Catalyst 2912MF XL
Embedded RMON	History, Events, Alarms, Statistics	Same as Catalyst 2912MF XL
Dimensions (HxWxD)	3.46 x 17.5 x 12 in. (8.8 x 44.5 x 30.5 cm)	3Same as Catalyst 2912MF XL
Weight	13.5 lb (6.12 kg); 15 lb (6.8 kg) with two modules installed	Same as Catalyst 2912MF XL

Selected Part Numbers and Ordering Information[1]

Catalyst 2900 Series XL Switches	
WS-C2912MF-XL	12-port 100BASE-FX, 2 module slots
WS-C2924M-XL-EN	24-port 10/100 (autosensing), 2 module slots
WS-C2924M-XL-EN-DC	24-port 10/100 (autosensing), 2 module slots, DC powered
Catalyst 2900 Series XL Switch Bundles	
WS-C2924M-XL-EN-5P	Five Catalyst 2924M XL Switches
Catalyst 2900 Series XL Modules	
WS-X2914-XL-V	4-port 10/100 ISL/802.1Q Module
WS-X2924-XL-V	4-port 100BASE-FX ISL/802.1Q Module
WS-X2922-XL-V	2-port 100BASE-FX ISL/802.1Q Module
WS-X2931-XL	1-port, GBIC-based, 1000BASE-X Switch Uplink Module
WS-X2932-XL	1-port 1000BASE-T Switch Uplink Module
WS-X3500-XL	GigaStack GBIC
WS-G5484=	SX GBIC; 1000BASE-SX short wavelength, multimode fiber
WS-G5486=	LX GBIC; 1000BASE-LX/LH, long wavelength/long haul, single or multimode fiber
Catalyst 2900 Series XL Accessories	
CAB-GS-1M	1 meter cable for GigaStack GBIC
CAB-GS-50CM	50 centimeter cable for GigaStack GBIC

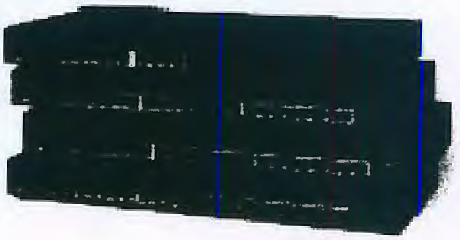
Catalyst 2900 Series XL Packaged SMARTnet Maintenance 8x5xNBD	
CON-SNT-PKG4	Catalyst 2900 Series WSC2924M-XL-EN Packaged SMARTnet 8x5xNBD
CON-SNT-PKG5	Catalyst 2900 Series WSC2924M-XL-EN-DC Packaged SMARTnet 8x5xNBD
CON-SNT-PKG7	Catalyst 2900 Series WSC2912MF-XL Packaged SMARTnet 8x5xNBD

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 2900 Series XL Web site: **http://www.cisco.com/go/2900xl**

Cisco Catalyst 2950 Series Intelligent Ethernet Switches



The Catalyst 2950 Series with Intelligent Ethernet Switches are fixed-configuration, standalone and stackable models that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity for small, mid-sized, service provider and industrial networks. The 2950C-24, 2950T-24, 2950G-12-EI, 2950G-24-EI, 2950G-48-EI and 2950G-24-EI-DC are part of an affordable product line that brings intelligent services, such as advanced quality of service, rate-limiting, security filters, and multicast management, to the network edge-while maintaining the simplicity of traditional LAN switching. When a Catalyst 2950 Switch is combined with a Catalyst 3550 Series Switch, the solution is capable of enabling IP routing from the edge to the core of the network. These Intelligent Ethernet Switches come with Enhanced Image (EI) software configuration only.

In addition to the range of Intelligent Ethernet switches, the Catalyst 2950 Series also includes switches with Standard Image (SI) software configuration only. The Cisco Catalyst 2950SX-24, 2950-24 and 2950-12, members of the Cisco Catalyst 2950 Series Switches, are standalone, fixed-configuration, managed 10/100 switches with Gigabit uplinks (2950SX-24 only) providing user connectivity for small to mid-sized networks. These wire-speed desktop switches come with Standard Image (SI) software features and offer Cisco IOS functionality for basic data, video and voice services at the edge of the network.

The Catalyst 2950 Series also includes the Cisco Catalyst 2955T-12, 2955C-12, and 2955S-12. The Cisco Catalyst 2955 are industrial-grade switches that provide Fast Ethernet and Gigabit Ethernet connectivity for deployment in harsh environments. With a range of copper and fiber uplink options, the Catalyst 2955 operates in environments such as industrial networking solutions (industrial Ethernet deployments), intelligent transportation systems (ITSs), and transportation network solutions. It is also suitable for many military and utility market applications where the environmental conditions or suspended solid concentrations exceed the specifications of other commercial switching products.

Embedded in all the products in the Catalyst 2950 Series is the Cisco Cluster Management Suite (CMS) Software, which allows users to simultaneously configure and troubleshoot multiple Catalyst desktop switches using a standard Web browser.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 2950 Series Intelligent Ethernet Switches with Enhanced Image (EI)	• Layer 2/3/4 based services: Advanced QoS, Security, High availability and STP enhancements • Wire-speed performance • Advanced QoS, Security, High availability and STP enhancements • Cisco Cluster Management • Stackable • GBIC based uplink ports for media flexibility
Catalyst 2950G-48-EI	• Ideal for desktop connectivity • High Port Density
Catalyst 2950G-24-EI	• Ideal for desktop connectivity • Medium Port Density
Catalyst 2950G-24-EI-DC	• Ideal for Telco/DCN environments • NEBS compliant • Medium Port Density
Catalyst 2950G-12-EI	• Ideal for desktop connectivity • Low Port density
Catalyst 2950T-24	• High speed uplink flexibility with fixed 10/100/1000BaseT ports • Low price per port
Catalyst 2950C-24	• High speed uplink flexibility over extended distances with fixed 100BASE-FX connections using MT-RJ connectors • Low price per port
Catalyst 2950 Series with Standard Image (SI)	• Wire speed, high performance switches for delivering 10/100 Mbps speed connectivity to desktop PCs, servers and other systems • Layer 2-based QoS and Security features • Cisco Cluster Management • Ideal for desktop connectivity
Catalyst 2950-12	• Low Port density
Catalyst 2950-24	• Medium port density
Catalyst 2950SX-24	• High speed uplinks with 2 fixed 1000BaseSX ports • Medium port density
Catalyst 2955 Series with Enhanced Image (EI)	• Ideal for harsh network environments • Rugged: Implements industrial-grade components, a compact form factor, convection cooling, and relay output signaling. Designed to operate at extreme temperatures and under extreme vibration and shock. • Layer 2/3/4 based services: Advanced QoS, Security, High availability and STP enhancements • Wire-speed performance
Catalyst 2955T-12	• Twelve 10/100 ports and two 10/100/1000BASE-TX (Copper) uplnks
Catalyst 2955C-12	• Twelve 10/100 ports and two 100BASE-FX (Multimode Fiber) uplinks
Catalyst 2955S-12	• Twelve 10/100 ports and two 100BASE-LX (Singlemode Fiber) uplinks

Key Features

- Cisco Cluster Management (CMS) Software offers superior manageability, ease-of-use and ease-of-deployment and enhanced configuration wizards
- Wire-speed performance in connecting end-stations to the LAN
- Catalyst 2950: Ideal for small- and mid-sized networks
- Catalyst 2955: Ideal for harsh network environments
- Sophisticated Multicast Management via IGMP Snooping
- Scalability and high availability features
- Support for Cisco Redundant Power System 300 (RPS 300)
- Switches with Standard Image (SI) include these additional features:
  - Catalyst 2950SX-24 switch provides a cost-effective solution for Gigabit speeds over fiber, offering 2 1000BaseSX uplinks
  - QoS and Security based on Layer 2 information
  - Basic Cisco IOS Services

- Intelligent Ethernet Switches with Enhanced Image (EI) include these additional features:
  - Catalyst 2950T-24 switch is a component of the Cisco Gigabit Ethernet over copper solution, offering 10/100/1000BaseT uplinks
  - Powerful Gigabit-uplink options—GBIC-based or 1000BaseT
  - Superior control through advanced intelligent services—advanced quality of service based on Layer 2 through Layer 4 parameters
  - Superior Security features: based on Layer 2 through Layer 4 Access Control Parameters
  - Enhanced Cisco IOS Services

Competitive Products

- Hewlett Packard: Procurve 2500 /2650
- Nortel: BPS 2000/450T/420T
- 3 Com: Superstack 3300/4300/4400/4400SE/4200 series
- Extreme: Summit 24 e2e3
- Dell: Powerconnect3024/3048/3248
- Hirshchmann
- GarretCom
- Sixnet

Specifications

Feature	Catalyst 2950G-48-EI	Catalyst 2950G-24-EI	Catalyst 2950G-24-EI-DC	Catalyst 2950G-12-EI	Catalyst 2950T-24
Fixed Ports	48 port 10/100 autosensing & 2 GBIC-based Gigabit Ethernet ports	24 port 10/100 autosensing & 2 GBIC ports	24 port 10/100 autosensing & 2GBIC ports and DC Power	12 port 10/100 autosensing & 2GBIC ports	26-port (24 10/100 autosensing & 2 ports 1000BaseT
Forwarding Bandwidth	13.6 Gbps	8.8 Gbps	8.8Gbps	6.4Gbps	8.8 Gbps
Forwarding Rate	10.1 Mpps	6.6 Mpps	6.6 Mpps	4.8 Mpps	6.6 Mpps
Full-Duplex Capabilities	All Ports	All Ports	All Ports	All Ports	All Ports
VLAN Maximum	250-port-based VLANS	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
FEC	Yes	Yes	Yes	Yes	Yes
802.1Q	Yes	Yes	Yes	Yes	Yes
Security	Port Security, with MAC aging, Private VLAN Edge, ACL, 802.11x, IBNS, SSH, RADIUS, TACACS+, SNMPv3 (crypto)	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
Multicast	IGMP Snooping	IGMP Snooping	IGMP Snooping	IGMP Snooping	IGMP Snooping
QoS	802.1P, 4 egress queues, WRR, SPS, Expedite Queuing, Policing, Marking, Layer 3 and 4 Services, Auto QoS	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
Management Capabilities	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
Software Image	Enhanced Image (EI)	Enhanced Image (EI)	Enhanced Image (EI)	Enhanced Image (EI)	Enhanced Image (EI)
Flash Memory	8 MB	8 MB	8 MB	8 MB	8 MB
CPU DRAM	16 MB	16 MB	16 MB	16 MB	16 MB
Embedded RMON	History, Events, Alarms, Statistics	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
Dimensions (H x W x D)	1.72 x 17.5 x 13 in.	1.72 x 17.5 x 9.52 in.	1.72 x 17.5 x 9.52 in.	1.72 x 17.5 x 9.52 in.	1.75 x 17.5 x 16 in.

Feature	Catalyst 2950C-24	Catalyst 2950-24	Catalyst 2950-12	Catalyst 2950SX-24	Catalyst 2955 (T-12,C-12,S-12)
Fixed Ports	26-port (24 10/100 autosensing & 2 ports100BaseFX)	24-port 10/100 autosensing	12-port 10/100 autosensing	26-port (24 10/100 autosensing & 2 ports1000BaseSX)	12 10/100 ports T-12: 2 fixed 10/100/1000BASE-T uplink ports C-12:2 fixed 100BASE-FX multimode uplink ports S-12: 2 fixed 100BASE-LX single-mode uplink ports
Forward Bandwidth	5.2 Gbps	4.8 Gbps	2.4 Gbps	8.8 Gbps	13.6 Gbps
Forwarding Rate	3.9 Mpps	3.6 Mpps	1.8 Mpps	6.6 Mpps	2 Mpps
Full-Duplex Capabilities	All Ports	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	All Ports
VLAN Maximum	250-port-based VLANS	64-port-based VLANS	64-port-based VLANS	64-port-based VLANS	250-port-based VLANS
FEC	Yes	Yes	Yes	Yes	Yes
802.1Q	Yes	Yes	Yes	Yes	Yes
Security	Port Security, with MAC aging, Private VLAN Edge, ACL, 802.11x, IBNS, SSH, RADIUS, TACACS+, SNMPv3 (crypto)	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	Port Security, with MAC aging, Private VLAN Edge, 802.11x, RADIUS, TACACS+, SNMPv3 (non-crypto)
Multicast	IGMP Snooping	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24
QoS	802.1P, 4 egress queues, WRR, SPS, Expedite Queuing, Policing, Marking, Layer 3 and 4 Services, Auto QoS	802.1P, 4 egress queues, WRR	802.1P, 4 egress queues, WRR	802.1P, 4 egress queues, WRR	802.1P, 4 egress queues, WRR
Management Capabilities	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS
Software Image	Enhanced Image (EI)	Standard Image (SI)	Standard Image (SI)	Standard Image (SI)	Enhanced Image(EI)
Flash Memory	8 MB	8 MB	8 MB	8 MB	16 MB
CPU DRAM	16 MB	16 MB	16 MB	16 MB	32 MB
Embedded RMON	History, Events, Alarms, Statistics	HSame as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	History, Events, Alarms, Statistics
Dimensions (H x W x D)	1.75 x 17.5 x 11.8 in.	1.75 x 17.5 x 11.8 in.	1.75 x 17.5 x 9.52 in.	1.75 x 17.5 x 9.52 in.	3.78x8.07x5.03in; connectorsfacing forward OR 5.03x8.07x3.78in; connectorsfacing downward

Selected Part Numbers and Ordering Information[1]

Catalyst 2950 Series Switches	
WS-C2950G-48-EI	Catalyst 2950G-48 switch with 48 10/100 ports and 2 Gigabit Interface Converter (GBIC)based GE ports
WS-C2950G-24-EI	Catalyst 2950G-24 switch with 24 10/100 ports and 2 GBIC ports
WS-C2950G-24-EI-DC	Catalyst 2950G-24-DC switch with 24 10/100 ports, 2 GBIC ports and DC Power
WS-C2950G-12-EI	Catalyst 2950G-12 switch with 12 10/100 ports and 2 GBIC ports
WS-C2950T-24	Catalyst 2950C-24T switch with 24 10/100 ports and two fixed 1000BaseT Uplink ports
WS-C2950C-24	Catalyst 2950C-24 switch with 24 10/100 ports and two fixed 100BaseFX Uplink ports
WS-C2950-24	Catalyst 2950-24 switch with 24 10/100 ports
WS-C2950-12	Catalyst 2950-12 switch with 12 10/100 ports
WS-C2950SX-24	Catalyst 2950SX-24 switch with 24 10/00 ports and two fixed 1000BaseSX Uplink ports
Gigabit Interface Converters (GBICs)	
WS-X3500-XL	GigaStack GBIC Gigabit Ethernet stacking GBIC and 50cm cable
WS-G5484=	1000BaseSX GBIC short wavelength GBIC (multimode fiberonly)
WS-G5486=	1000BaseLX/LH GBIC long wavelength/long haul GBIC (single or multimode fiber)
WS-G5487=	1000BaseZX GBIC extended-reach GBIC (singe mode fiber only)
WS-G5483=	1000BaseT GBIC- Gigabit-Ethernet-over-copper GBIC

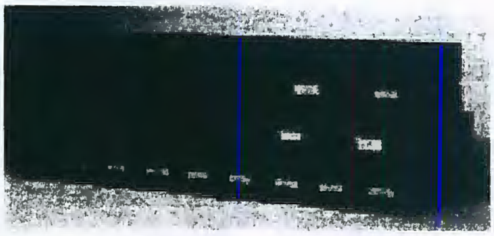
Redundant Power System (RPS)	
PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable
CAB-RPS-1414=	1.2 meter cable for CiscoRPS 300to external device connection
Cables/Accessories	
CAB-RPS-1614=	1 RPS 675 connector cable 16/14
CAB-GS-50CM	50 centimeter cable for GigaStack GBIC
STK-RACKMOUNT-1RU=	Rack mount kit for 1 RU versions of Catalyst 2950, 3500 XL, 2900 XL, 1900, and FastHub 400 switches
Packaged SMARTnet 8x5xNBD Maintenance Contract	
CON-SNT-PKG3	Packaged SMARTnet 8x5xNBD Maintenance forthe Catalyst 2950G-12, 2950-24 and 2950-12
CON-SNT-PKG4	Packaged SMARTnet8x5xNBD Maintenance forthe Catalyst 2950G-24 and 2850G-24-DC
CON-SNT-PKG6	Packaged SMARTnet 8x5xNBD Maintenance forthe Catalyst 2950G-48

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 2950 Series Web site: **http://www.cisco.com/go/catalyst2950**

Cisco Catalyst 3500 Series XL



The Cisco Systems Catalyst 3500 series XL is a scalable line of stackable 10/100 and Gigabit Ethernet switches that delivers premium performance, flexibility, and manageability with unparalleled investment protection. This line of low-cost, high-performance switching solutions provides next-generation stackable switching through an independent high-speed stacking bus that preserves valuable desktop ports. Cisco's breakthrough Switch Clustering technology expands the stacking domain beyond a single wiring closet, enabling up to 16 interconnected Catalyst 3550, 2950, 3500 XL, 2950, 2900 XL and 1900 switches—regardless of geographic location—to form a flexible, single IP managed network.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 3524-PWR XL	• A stackable, wire-speed 10/100 and Gigabit Ethernet switch for delivering dedicated 10 or 100 Mbps to individual users and servers • Advanced QoS, high avalability, and integrated in-line power enabling easy deployment of IP phones and wireless access points.
Catalyst 3508G XL	• A stackable Gigabit Ethernet switch with eight GBIC-based portsfor aggregating a groupof Gigabit Ethernet switches and servers through Cisco GigaStack GBICs or standard 1000BASE-X GBICs • Dedicated, high-speed Gigabit Ethernet performance

Key Features

- 10.8 Gbps switch fabric, up to 8 Mpps forwarding rate, and maximum forwarding bandwidth of 5.4 Gbps across all 10/100 ports
- Built-in Gigabit Ethernet ports accommodate a range of GBIC transceivers, including the Cisco GigaStack GBIC, 1000BASE-T, 1000BASE-SX and 1000BASE-LX/LH GBICs, and 1000BASE-ZX extended reach GBIC
- Low-cost, 2-port Cisco GigaStack GBIC offers a range of configurable stacking and performance options by delivering 1-Gbps connectivity in a daisy-chained connection or up to 2-Gbps in a dedicated, switch-to-switch connection
- Support for IEEE 802.1p technology for prioritization of mission-critical and time-sensitive application such as voice and telephony traffic
- 3524-PWR XL provides in-line power to IP phones and other devices

Competitive Products

- 3Com: SuperStack 3Switch 3300 and 3900
- Hewlett Packard: ProCurve 2524, 2424M, 4000, and 8000
- Nortel: BayStack 450T and BPS 2000 switches

Specifications

Feature	Catalyst 3524-PWR XL	Catalyst 3508G XL
Fixed Ports	24-port 10/100 autosensing 2-port 1000BASE-X (GBIC)	8-port 1000BASE-X (GBIC)
Modular Slots	None	None
Backplane	10 Gbps	10 Gbps
Stackable	Yes	Yes
Full-Duplex	All ports	All ports
VLAN Maximum	250 port-based VLANs or ISL/802.1Q trucks	250 port-based VLANs or ISL/802.1Q trucks
FEC	Yes	Yes
Inter-Switch Link	Yes	Yes
In-Line Power	Yes	No
Management Capabilities	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded Cisco Visual Switch Manager, Web-based interface	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded Cisco Visual Switch Manager, Web-based interface
Processors	Cisco designed ASICs	Cisco designed ASICs
Flash Memory	4 MB	4 MB
CPU DRAM	8 MB	8 MB
Embedded RMON	History, Events, Alarms, Statistics	History, Events, Alams, Statistics
Dimensions (HxWxD)	1.75 x 17.5 x 11.8 in	1.75 x 17.5 x 11.8 in

Selected Part Numbers and Ordering Information[1]

Catalyst 3500 Series XL Switches	
WS-C3524-PWR-XL-EN	24-port 10/100 (autosensing), 2 1000X GBIC Slots, inline power
WS-C3508G-XL-EN	8 1000X GBIC Slots
Catalyst 3500 Series XL Accessories	
WS-X3500-XL	GigaStack GBIC
WS-G5484=	1000BASE-SX GBIC
WS-G5486=	1000BASE- LX/LH GBIC
WS-G5487=	1000BASE- ZX extended reach GBIC
WS-G5483=	1000BASE-T GBIC
Catalyst 3500 Series XL Basic Maintenance	
CON-SNT-PKG4	Catalyst 3512 XL SMARTnet 8x5xNBD Maintenance
CON-SNT-PKG5	Catalyst 3524 XL and 3524-PWR XL SMARTnet 8x5xNBD Maintenance
CON-SNT-PKG6	Catalyst 3548 XL SMARTnet 8x5xNBD Maintenance
CON-SNT-PKG9	Catalyst 3508G XL SMARTnet 8x5xNBD Maintenance

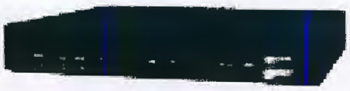
[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 3500 series XL Web site: **http://www.cisco.com/go/3500xl**

804

Cisco Catalyst 3550 Series Intelligent Ethernet Switches



The Cisco Catalyst 3550 Series Intelligent Ethernet Switches is a line of enterprise-class, stackable, multilayer switches that provide high availability, scalability, security and control to enhance the operation of the network. With a range of Fast Ethernet and Gigabit Ethernet configurations, the Catalyst 3550 Series can serve as both a powerful access layer switch for medium enterprise wiring closets and as a backbone switch for small networks. Now customers can deploy network-wide intelligent services, such as advanced quality of service, rate-limiting, Cisco security access control lists, multicast management, and high-performance IP routing—while maintaining the traditional LAN switching.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 3550 Series	• Enterprise-class intelligent services such as ACLs, advanced QoS, and rate-limiting • Cisco Cluster Management
Catalyst 3550-48-EMI (Enhanced Multilayer Software Image)	• High performance advancedIP routing • High Port Density • Ideal as a powerful access layer switch for a medium enterprise wiring closet with routed uplinks
Catalyst 3550-48-SMI (Standard Multilayer Software Image)	• High Port Density • Ideal for a powerful access layer switch for a medium enterprise wiring closet • Basic IP routing
Catalyst 3550-24-EMI (Enhanced Multilayer Software Image)	• High performance advancedIP routing • Medium Port Density • Ideal for a powerful access layer switch for a medium enterprise wiring closet with routed uplinks
Catalyst 3550-24-SMI (Standard Multilayer Software Image)	• Medium Port Density • Ideal for a powerful access layer switch for a medium enterprise wiring closet • Basic IP routing
Catalyst 3550-24PWR-EMI (Enhanced Multilayer Software Image)	• High performance advancedIP routing • Medium Port Density • Integrated inlinepower to Cisco IP telephones and Cisco wireless LAN access points • Ideal for a powerful access layer switch for a medium enterprise wiring closet with routed uplinks
Catalyst 3550-24PWR-SMI (Standard Multilayer Software Image)	• Medium Port Density • Integrated inlinepower to Cisco IP telephones and Cisco wireless LAN access points • Ideal for a powerful access layer switch for a medium enterprise wiring closet • Basic IP routing
Catalyst 3550-24-DC-SMI (Standard Multilayer Software Image)	• Medium Port Density • DC powered, NEBS level 3 compliant • Basic IP routing
Catalyst 3550-24-FX-SMI (Standard Multilayer Software Image)	• Medium Port Density • Ideal for 100FX aggregation • Basic IP routing
Catalyst 3550-12G	• High performance IP routing • Gigabit Ethernet aggregation using fiber • Ideal for stack aggregation, server aggregation, or as a backbone switch in a mid-sized network
Catalyst 3550-12T	• High performance advancedIP routing • Gigabit Ethernet aggregation using Category 5 copper cabling • Ideal for stack aggregation, server aggregation, or as a backbone switch in a mid-sized network
CD-3550-EMI	• High performance advancedIP routing • EMI upgrade kit for standardversions of the Catalyst 3550-24, 3550-24 PWR, 3550-24-DC, 3550-24-FX, and 3550-48 switches

Key Features

- Network control and bandwidth optimization via advanced Quality of Service (QoS), granular rate-limiting, Access Control Lists (ACLs), and multicast services
- Network security through a wide range of authentication methods, data encryption technologies, and access restriction features based on users, ports, and MAC addresses
- Network scalability through advanced routing protocols such as EIGRP, OSPF, BGP, and PIM (requires Enhanced Multilayer Software Image (EMI))
- Intelligent adaptability through Cisco Identity Based Networking Services (IBNS) offering greater flexibility and mobility to stratified users
- Lower Total Cost of Ownership (TCO) for IP Telephony and Wireless LAN deployments through integrated inline power (Catalyst 3550-24 PWR only)
- Easy switch configuration and deployment of advanced services through the embedded Cluster Management Suite (CMS) Software
- Stackable up to 9 switches with the Gigastack GBIC

Competitive Products

- Extreme Networks: Summit5i, Summit 24/48, Summit 48i
- Foundry: FastIron 4802
- Nortel: BPS 2000

Specifications

Feature	Catalyst 3550-48	Catalyst 3550-24	Catalyst 3550-24PWR	Catalyst 3550-12G	Catalyst 3550-12T	Catalyst 3550-24-DC	Catalyst 3550-24-FX
Fixed Ports	48 10/100 ports 2 GBIC-based Gigabit Ethernet ports	24 10/100 ports 2 GBIC-based Gigabit Ethernet ports	24 10/100 ports 2 GBIC-based Gigabit Ethernet ports	10 GBIC-based Gigabit Ethernet ports 2 10/100/1000 ports	10 10/100/1000 ports 2 GBIC-based Gigabit Ethernet ports	24 10/100 ports2 GBIC-based Gigabit Ethernet port	24 100FX MMF ports 2 GBIC-based Gigabit Ethernet port
Switching Fabric	13.6 Gbps	8.8 Gbps	8.8 Gbps	24 Gbps	24 Gbps	8.8 Gbps	8.8 Gbps
VLAN Maximum	1005	1005	1005	1005	1005	1005	1005
FEC/GEC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GBICs	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX, CWDM	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX
802.1Q and ISL	Yes	Yes	Yes	Yes	Yes	Yes	Yes
In-Line Power	No	No	No	No	No	No	No
QoS	802.1p, DSCP, 4 egress Queues, WRR, Strict Priority Queui.ıg,WRED	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48
Multicast	IGMP Snooping, PIM (requires EMI), DVMRP (requires EMI), CGMP Server (requires EMI)	IGMP Snooping, PIM (requires EMI), DVMRP (requires EMI), CGMP Server (requires EMI)	IGMP Snooping, PIM (requiresEMI), DVMRP (requires EMI), CGMP Server (requires EMI)	IGMP Snooping, PIM, DVMRP, CGMP Server	IGMP Snooping, PIM, DVMRP, CGMP Server	IGMP Snooping, PIM (requires EMI), DVMRP (requires EMI), CGMP Server (requires EMI)	IGMP Snooping, PIM (requires EMI), DVMRP (requires EMI), CGMP Server (requires EMI)
Management Capabilities	SNMP, Telnet, RMON, CWSI, CLI-based out-of-band, embedded CMS	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48
Flash Memory	16 MB	16 MB	16 MB	16 MB	16 MB	16 MB	16 MB
CPU DRAM	64 MB	64 MB	64 MB	64 MB	64 MB	64 MB	64 MB

Feature	Catalyst 3550-48	Catalyst 3550-24	Catalyst 3550-24PWR	Catalyst 3550-12G	Catalyst 3550-12T	Catalyst 3550-24-DC	Catalyst 3550-24-FX
Embedded RMON	History, Events, Alarms, Statistics	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48
Dimensions (H x W x D)	1.75 x 17.5 x 16.3 in.	1.75 x 17.5 x 14.4 in.	1.75 x 17.5 x 17.4 in.	2.63 x 17.5 x 15.9 in.	2.63 x 17.5 x 15.9 in	1.75 x 17.5 x 14.4 in.	1.75 x 17.5 x 16.3 in.

Selected Part Numbers and Ordering Information[1]

Catalyst 3550 Series Intelligent Ethernet Switches

WS-C3550-48-SMI	Catalyst 3550-48 multilayer switch with 48 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; SMI installed
WS-C3550-48-EMI	Catalyst 3550-48 multilayer switch with 48 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; EMI installed
WS-C3550-24-SMI	Catalyst 3550-24 multilayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; SMI installed
WS-C3550-24-EMI	Catalyst 3550-24 multilayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; EMI installed
WS-C3550-24PWR-SMI	Catalyst 3550-24 multilayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; integrated inline power; SMI installed
WS-C3550-24PWR-EMI	Catalyst 3550-24 multilayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; integrated inline power; EMI installed
WS-C3550-24-DC-SMI	Catalyst 3550-24-DC multiplayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernetports; SMI installed; DC-powered
WS-C3550-24-FX-SMI	Catalyst 3550-24-FX multilayer switch with 24100FX multimode fiber ports and 2 GBIC-based Gigabit Ethernet ports; SMI installed
WS-C3550-12G	10 GBIC-based Gigabit Ethernet ports and 2 10/100/1000 ports; EMI installed
WS-C3550-12T	10-10/100/1000BaseT ports and 2 GBIC-based Gigabit Ethernet ports; EMI installed
CD-3550-EMI=	EMI upgrade kit for the standard versions of the Catalyst 3550-24, 3550-48, 3550-24PWR, 3550-24-DC, and 3550-24-FX

Gigabit Interface Converters (GBICs)

WS-X3500-XL	GigaStack Stacking GBIC and 50 cm cable
WS-G5484=	1000BaseSX GBIC-short wavelength GBIC (multimodefiber only)
WS-G5486=	1000BaseLX/LH GBIC-long wavelength/long haul GBIC (single or multimode fiber)
WS-G5487=	1000BaseZX GBIC-extended reach GBIC (singlemode fiber only)
WS-G5483=	1000BaseT GBIC-Gigabit Ethernetover Copper GBIC

Redundant Power System (RPS)

PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable
VAB-RPS-1414=	1.2 meter cable for Cisco RPS 300 to external device connection

Cables/Accessories and Redundant Power Supply

CAB-RPS-1614=	1 RPS 675 connector cable 16/14
RCKMNT-3550-1.5RU=	Rack mount kit for the Catalyst 3550-12T and 3550-12G switches
RCKMNT-1RU=	Rack mount kit for the Catalyst 3550-24, 3550-48, 3550-24PWR, 3550-24-DC, and 3550-24-FX switches

Packaged SMARTnet 8x5xNBD Maintenance Contract for Two-Tier Customers

CON-SNT-PKG9	Packaged SMARTnet 8x5xNBD for the WS-C3550-12T and WS-C3550-12G
CON-SNT-PKG4	Packaged SMARTnet 8x5xNBD for the WS-C3550-24-SMI and WS-C3550-24PWR-SMI
CON-SNT-PKG5	Packaged SMARTnet 8x5xNBD for the WS-C3550-24-DC-SMI
CON-SNT-PKG6	Packaged SMARTnet 8x5xNBD for the WS-C3550-24-EMI, WS-C3550-24PWR-SMI and WS-C3550-48-SMI
CON-SNT-PKG7	Packaged SMARTnet 8x5xNBD for the WS-C3550-48-EMI and WS-C3550-24-FX-SMI

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 3550 Series Web site: **http://www.cisco.com/go/cat3550**

Cisco Catalyst 4500 Series

The Cisco Catalyst 4500 Series integrates nonblocking Layer 2/3/4 switching with optimal control, enabling business resilience for enterprise and metropolitan Ethernet customers deploying Internet-based business applications. A next generation Catalyst 4000 Series platform, the Cisco Catalyst 4500 Series includes three new chassis: Catalyst 4507R (7-slot: redundant Supervisor IV capable), Catalyst 4506 (6-slot) and Catalyst 4503 (3-slot). A key component of Cisco AVVID (Architecture for Voice, Video and Integrated Data), the Catalyst 4500 extends control to Enterprise wiring closets, branch office and Layer 3 distribution points. A variety of network infrastructure solutions are enabled by the Catalyst 4500 Series of switches including: Cisco IOS Network Services, IP Telephony, 10/100/1000 to the desktop, Wireless LAN, NetFlow Services and Metro Ethernet Switching.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 4507R	• When network resiliency via redundant Supervisor Engines is crucial to customer success • Port density up to 240-10/100, 100-FX, or 10/100/1000BASE-T with modular investment protection • Layer 2 and Layer 3 Cisco Express Forwarding (CEF)-based switching up to 64 Gbps, 48 Mpps
Catalyst 4506	• Port density up to 240-10/100, 100-FX, or 10/100/1000BASE-T with modular investment protection • Layer 2 and Layer 3 Cisco Express Forwarding (CEF)-based switching up to 64 Gbps, 48 Mpps
Catalyst 4503	• Port density up to 96-10/100, 100-FX, or 10/100/1000BASE-T with modular investment protection • Layer 2 and Layer 3 Cisco Express Forwarding (CEF)-based switching up to 28 Gbps, 21 Mpps

Note: Compatible sparing between Catalyst 4507R, 4506, and 4503 chassis provides investment protection with common power supplies and switching line cards. The Catalyst 4500 series also leverages the same feature set with identical software code base along with the same enterprise functionality as the Catalyst 6500 Series in the wiring closet, delivering a consistent end-to-end solution.

Key Features

- Supervisor II
  - Catalyst 4500/6500 Series CatOS Software, single IPQ—Address Management, and security (TACACS+, port lockdown, RADIUS, Kerberos)
  - Enterprise VLANs (4,096) with 802.1Q support on all ports, 16,000 MAC Addresses, and Spanning-Tree Protocol (802.1D) enhancements (UplinkFast, PortFast, and BackboneFast) for deterministic/fast failover
  - Fast and Gigabit EtherChannel aggregation (up to 8 Gbps full duplex), load balancing and failover on every port, and port filtering
- Supervisor IV
  - Capable of 1+1 redundancy in a 4507R (Single Supervisor only in Catalyst 4506 and 4503)
  - Optional NetFlow Services Card Support
  - Integrated Layer 2/3/4 CEF based switching at 64Gbps and 48Mpps
  - Feature rich and proven Cisco IOS Software
  - Port based enhanced QOS with multiple queues (16k input; 16k output), bandwidth management, policing and Access Control Lists (16k input ACL entries; 16k output entries)
  - Enterprise VLANs (4,000) with 802.1Q and ISL support on all ports, 32,000 MAC Addresses, and Spanning-Tree Protocol (802.1D), 802.3w, 802.3s

- Supports RIP I, RIP II, Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP) Enhanced IGRP (EIGRP), BGP4, IS:IS, Software based IPX and Appletalk, Hot Standby Router Protocol (HSRP), Cisco Group Management Protocol (CGMP), IGMP v1 and II, Internet Control Message Protocol (ICMP), and both Protocol Independent Multicast (PIM) sparse and dense modes, and Distance Vector Multicast Routing Protocol (DVMRP) interoperability
- Optional compact flash memory cards

Competitive Products

- Extreme Networks: Alpine 3802, Alpine 3804, and Alpine 3808
- Enterasys: Matrix E-5, Matrix E-6, Matrix E-7
- Foundry: FastIron 400/800, FastIron II, II+, III, BigIron4000
- Hewlett Packard: Procurve 5300XL, 4108GL
- Nortel: Passport 8100

Specifications

Feature	Catalyst 4507R	Catalyst 4506	Catalyst 4503
Fixed Ports	2 Gigabit uplinkports on Supervisor IV	2 Gigabit uplink ports on Supervisor Engine II, III and Supervisor IV	2 Gigabit uplinkports on Supervisor Engine II, IIIand Supervisor IV
Maximum Port Density	240 (10/100 Fast Ethernet) 240 (100-FX Fast Ethernet) 240 (10/100/1000BASE-T)	240 (10/100 Fast Ethernet) 240 (100-FX Fast Ethernet) 240 (10/100/1000BASE-T)	96 (10/100 Fast Ethernet) 96 (100-FX Fast Ethernet) 96 (10/100/1000BASE-T)
Modular Slots	7 (2 for Supervisors	6 (1 for Supervisor)	3 (1 for Supervisor)
Available Modules	Supervisor Engine IV	Supervisor Engine II, III, and IV	Supervisor Engine II, III, and IV
Redundant Supervisor Capable	Yes	No	No
Backplane Capacity	64 Gbps	64 Gbps	28 Gbps
Stackable	No	No	No
Hot-Swappable Power Supplies	Yes (2 bays, 1+1)	Yes (2 bays, 1+1)	Yes (2 bays, 1+1)
Embedded RMON	Statistics, History, Alarm, Events	Statistics, History, Alarm, Events	Statistics, History, Alarm, Events
Dimensions (H x W x D)	19.19 x 17.31 x 12.50 in 48.74 x 43.97 x 31.70 cm	17.38 x 17.31 x 12.50 in 44.13 x 43.97 x 31.70 cm	12.25 x 17.31 x 12.50 in 31.12 x 43.97 x 31.70 cm

Selected Part Numbers and Ordering Information[1]

Catalyst 4500 Series Switches	
WS-C4507R	Catalyst 4500 Chassis (7-Slot),fan, no p/s, Red Sup Capable
WS-C4506	Catalyst 4500 Chassis (6-Slot),fan, no p/s
WS-C4503	Catalyst 4500 Chassis (3-Slot),fan, no p/s
Catalyst 4500 Series Common Equipment	
WS-X4013=	Catalyst 4000 Supervisor Engine II, Console(RJ-45), Mgt. (RJ-45) (Spare)
WS-X4014=	Catalyst 4000 Supervisor III (2 GE), Console(RJ45)
WS-X4515=	Catalyst 4000 Supervisor IV, 2 GE, Console(RJ-45)
WS-F4531=	Catalyst 4000 NetFlow Services card for Supervisor Engine IV
PWR-C45-1000AC=	Catalyst 4500 1000W AC Power Supply(Data Only)
PWR-C45-1300ACV=	Catalyst 4500 1300W AC Power Supplywith Int Voice
PWR-C45-2800ACV=	Catalyst 4500 2800W AC Power Supplywith Int Voice
Catalyst 4000 Series Common Equipment	
WS-C4003-S1	Catalyst 4003 Chassis (3-Slot), Supervisor Engine 1, 1-AC Power Supply, Fan Tray, Rack-Mount Kit
WS-C4006-S2	Catalyst 4006 Chassis (6-Slot), Supervisor II, (2)AC Power Supplies,Fan Tray, Rack-Mount Kit
WS-C4006-S3	Catalyst 4006 Chassis (6-slot), Supervisor III, (2) AC Power Supplies, Fan Tray, Rack-Mount Kit
WS-C4006-S4	Catalyst 4006 Chassis (6-slot), Supervisor IV, (2) AC Power Supplies, Fan Tray, Rack-Mount Kit
WS-X4008=	Catalyst 4003/4006 AC Power Supply (Spare)
WS-X4095-PEM=	Catalyst 4000 DC Power Entry Module (Spare)
WS-P4603-2PSU	Catalyst 4000 Aux. Power Shelf with 2 PSU
WS-X4608=	Catalyst 4603 Power Supply Unit for WS-P4603

Catalyst 4500 Series Line Card Modules and GBICs	
WS-X4124-FX-MT=	Catalyst 4000 FE Switching Module, 24-port 100FX (MTRJ)
WS-X4148-FX-MT=	Catalyst 4000 FE Switching Module, 48-100FX MMF (MTRJ)
WS-X4148-RJ=	Catalyst 4000 10/100 Fast Ethernet Module, 48 Ports (RJ-45)
WS-X4148-RJ21=	Catalyst 4000 Telco switch module, 48-port 10/100 (4xRJ21)
WS-X4148-RJ45V=	Catalyst 4000 Inline Power 10/100, 48-port (RJ45)
WS-X4232-GB-RJ=	Catalyst 4000 E/FE/GE Module, 2-GE (GBIC), 32-10/100 FE (RJ-45)
WS-X4232-RJ-XX=	Catalyst 4000 FE Base Module, 32-10/100(RJ45)+ Modular Uplink slot
WS-X4232-L3=	Catalyst 4000 E/FE/GE L3 Module, 2-GE(GBIC), 32-10/100 (RJ45)
WS-X4306-GB=	Catalyst 4000 Gigabit Ethernet Module, 6 Ports (GBIC)
WS-X4424-GB-RJ-45=	Catalyst 4000 24 port 10/100/1000 Auto-Sensing Module (RJ45)
WS-X4448-GB-RJ45=	Catalyst 4000 48 port 10/100/1000 Auto-Sensing Module (RJ45)
WS-X4418-GB=	Catalyst 4000 GE Module, Server Switching 18 Ports (GBIC)
WS-U4504-FX-MT=	Catalyst 4000 FE Uplink Daughter Card, 4-port 100FX (MTRJ)
WS-X4604-GWY=	Catalyst 4000 Access Gateway Module with IP/FW software
WS-G5483=	1000BASE-T GBIC (RJ-45)
WS-G5484=	1000BASE-SX Shortwave GBIC Module (Multimode Only)
WS-G5486=	1000BASE-LX/LH Long Haul GBIC Module (Multimode or Single Mode)
WS-G5487=	1000 BASE-ZX GBIC module (Single Mode Only)
Catalyst 4500 Series Software	
S4KL3-12113EW=	Cisco IOS BASIC L3 SW Cat4500 SUP 3/4(RIP,St.Routes,IPX,AT)
S4KL3E-12113EW=	Cisco IOS ENHANCED L3 SW Cat4500 SUP3/4(OSPF,IGRP,EIGRP,IS-IS)
SC4K-SUPK8-7.5.1=	Catalyst OS L2 SW Cat4500 Sup 2
WS-C4006-EMS-LIC	Catalyst 4006 RMON Agent License
WS-C4003-EMS-LIC	Catalyst 4003 RMON Agent License
Catalyst 4500 Series Basic Maintenance	
CON-SNT-PKG11	Catalyst 4003 SMARTnet 8x5xNBD Maintenance
CON-SNT-PKG12	Catalyst 4006 SMARTnet 8x5xNBD Maintenance

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 4500 series Web site: **http://www.cisco.com/go/cat4000**

Cisco Catalyst 4000 Series — Fixed Configuration

Cisco offers two dedicated Gigabit Ethernet fixed configuration switches; the Catalyst 4908G-L3 and the Catalyst 4912G. The Catalyst 4908G-L3 Switch is a fixed configuration Layer 3 Ethernet switch featuring wire-speed switching for IP, IPX and IP Multicast. It provides the high performance required for midsize campus backbones with optimum port density.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 4908G	• Cost effective dedicated Gigabit Ethernet Layer 3 backbone solution ideal for deployment in midsize networks for those customers who need wire speed Layer 3 performance but do not require Gigabit Ethernet density over 8 ports.
Catalyst 4912G	• Advanced wirespeed, non-blocking Layer 2 Gigabit Ethernet performance with intelligent Cisco IOS services and high-speed connections to workstations or servers; flexible Gigabit Interface Converter (GBIC) interfaces on all ports

Key Features

- Catalyst 4908G-L3:
  - 8 ports of 1000BASE x Gigabit Ethernet with GBIC support; Layer 3 switching and routing of IP, IPX and IP Multicast with wire speed Layer 2 switching for non routable protocols; Gigabit Etherchannel capability on every port
- Catalyst 4912G:
  - Wire-speed performance with 24 Gbps of dedicated bandwidth for nonblocking Gigabit Ethernet concentration, broad Gigabit EtherChannel availability, and GBIC flexibility on fiber port interfaces covering a wide range of cabling distances

Competitive Products

- Extreme Networks: Summit 1
- Foundry: Turbo Iron 8
- Nortel: Accellar 1200

Specifications

Feature	Catalyst 4908G-L3	Catalyst 4912G
Fixed Ports	8 (All Layer 3)	12 (All Layer 2)
Backplane Capacity	22 Gbps	24 Gbps
Stackable	No	No
VLAN Maximum	244	244
802.1Q	Yes	Yes
ISL	Yes	No
Menegement Capabilities	Inboard console via terminal or modem, outboard via Telnet, SNMP, CiscoView, CWSI, CiscoWorks 2000	Inboard console via terminal or modem, outboard via Telnet, SNMP, CiscoView, CWSI, CiscoWorks 2000
Dimensions (H x W x D)	2.69 x 17.1 x 18in	2.75 x 17.5 x 15 in.

Selected Part Numbers and Ordering Information[1]

Catalyst 4000 Switch Family

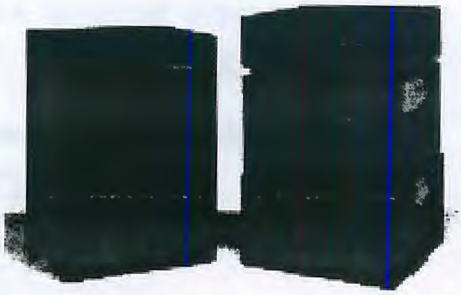
WS-4908G-L3	Catalyst 4908G-L3 switch
WS-C4912G	Catalyst 4912G switch, fixed 12-ports switched 1000BASE-X (GBIC)
WS-G5484=	1000BASE-SX GBIC module
WS-G5486=	1000BASE-LX/LH GBIC module
WS-G5487=	1000BASE-ZX GBIC module

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 4000 series Web site: **http://www.cisco.com/go/cat4000**

Cisco Catalyst 5000 Family



On October 4, 2002, Cisco Systems announced the end of sale for the Cisco Catalyst 5000 and 5500 series of modular switches, including all related Cisco Catalyst 5000 and 5500 series chassis and modules. The Cisco Catalyst 5000 and 5500 series chassis and modules will be orderable through June 30, 2003.

The Catalyst 5000 family features a Gigabit Ethernet and ATM-ready platform offering users high-speed trunking technologies, including Fast EtherChannel and OC-12 ATM. This series also provides a redundant architecture, dynamic VLANs, complete intranet services support, and media-rate performance with a broad variety of interface modules.

Migration Options

	When a Customer Needs These Features
Catalyst 6500 with Sup2/msfc2	• High Performance L3 wiring closet, data centre,or core feature sets • Integrated L2-7 Serices Modules • Layer 3 Routing Capabilities • Scalability to 256 Gbps • Hardware based QoS and ACLs • IOS software
Catalyst 6500 with Sup2/pfc2	• High Performance L2 wiring closet, data centreor core feature sets • Scalability to 256 Gbps • Hardware based QoS and ACLs
Catalyst 6500 with sup1A-2GE	• Low cost of entry wiring closet solution • Scalability to 32Gbps • Basic security and L2 QoS capabilities • L2 Stateful failover capabilities

Competitive Products

- Enterasys: Matrix E7, Expedition ER16
- Nortel: Passport 8100, 8600
- Extreme: Black Diamond
- Foundry: Big Iron

Specifications

Feature	Catalyst 5500	Catalyst 5505	Catalyst 5509
Modular Slots	13	5	9
Available Modules	Supervisor[1] Engine II G, III G, or III plus any combination of modules (subset listed under Part Numbersand Ordering Information)	Same as Catalyst 5500	Same as Catalyst 5500
Backplane	3.6 Gbps ATM switching: 5-Gbps backplane	3.6 Gbps	3.6 Gbps
Full-Duplex Capabilities	All Ethernet, Fast Ethernet, Token Ring, and ATM ports	Same as Catalyst 5500	Same as Catalyst 5500
VLAN Maximum	Spanning tree: Yes per VLAN 1000 VLANs	Same as Catalyst 5500	Same as Catalyst 5500
FEC	100BASE-TX; 100BASE-FX; 1000 BASE-X	Same as Catalyst 5500	Same as Catalyst 5500
Management Capabilities	Inboard console via terminal or modem, outboard via Telnet, SNMP, CiscoView, CWSIStatistics, history, alarms, events	Same as Catalyst 5500	Same as Catalyst 5500
Dimensions (HxWxD)	25.25 x 17.3 x 18.25 in.	10.4 x 17.2 x 18.14 in.	20 x 17.25 x 18.14 in.

[1] Supervisor module(s) require a slot in the chassis.

Selected Part Numbers and Ordering Information[1]

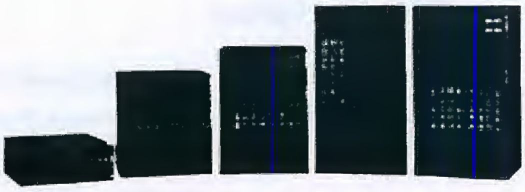
Catalyst 5000 Family Switch Families	
WS-C5507=	13-slot Chassis, AC Power Supply
WS-C5505-CHAC=	Catalyst 5505 Chassis, AC Power Supply
WS-C5509-CHAC=	Catalyst 5509 Spare Chassis, AC Power Supply
WS-C5509-CHDC=	Catalyst 5509 Spare Chassis, DC Power Supply
Catalyst 5000 Family Basic Maintenance	
CON-SNT-PKG13	Catalyst 5505 Packaged SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG16	Catalyst 5500 Packaged SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG15	Catalyst 5509 Packaged SMARTnet Maintenance 8x5xNBD

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 5500/5000 series Web site: **http://www.cisco.com/go/5000**

Cisco Catalyst 6500 Family



The Catalyst 6500 Family delivers highly available secure converged network services for the Enterprise and Service Provider networks. Designed to address the increased requirements for gigabit scalability, high-availability, rich services, and multilayer switching in backbone, distribution, and wiring closet topologies as well as datacenter environments, the Catalyst 6500 Family delivers exceptional scalability and price/performance, supporting a wide range of interface densities, performance, and integration of powerful service modules. The Catalyst Family delivers a wide range of intelligent switching solutions, enabling corporate intranets, extranets, and the internet for multimedia, mission-critical data, and voice applications.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 6500 Series	• A highly scalable platformthat meets requirements for a dynamic environment includingvery high multilayer switching performancewith high Fast Ethernet and Gigabit Ethernetport densities
Catalyst 6500 Family Solutions	• Enterprise campus distribution and core—Withindustry-leading port densities, performance, and high availability solutions • Enterprise Server Farm—For Gigabit wire-speed access to mission-critical server farms • High-capacitywiring closets—In very large deployments, the Catalyst 6000 family delivers advanced Layer 2, 3, and 4 switching in wiring closets • Value wiring closets where basic L2 QoS and ACL capabilities are required in addition to 2-3 Sec L2 Stateful failover • WAN/LAN/MAN integration—Single integated platform simplifiés networkdesign, decreases rack space requirements, and decreases overall administration costs • Advanced, integrated hardwae based firewall, contentswitching, intrusion detection, and network analysis capabilies • Service Provider Networks—For all dynamic environments including e-commerce, web hosting, and co-location facilities

Key Features

- Application-aware networking with multilayer switching intelligence and support for CiscoAssure policy networking
- High-availability features deliver maximum uptime for mission-critical application support
- Extensive Quality of Service (QOS) features to support mission-critical applications
- Scalable performance to 210 Mpps
- Maximum 10/100 Ethernet port density: 96 (3-slot chassis), 240 (6-slot chassis), 384 (9-slot chassis), and 576 (13-slot chassis)
- Maximum Gigabit Ethernet port density: 32 (3-slot chassis), 82 (6-slot chassis), 130 (9-slot chassis), and 194 (13-slot chassis)

Competitive Products

- Extreme: Black Diamond
- Foundry: Big Iron
- Lucent: Cajun Switch 550
- Nortel: Passport 8600

Specifications

Feature	6503	6506	6509	6513
Modular Slots	3	6	9	13
Available Modules	8 & 16 port Gigabit Ethernet 24 port 100FX Ethernet (multimode or single mode); 48 port 10/100TX Ethernet (RJ45); 48 port 10/100 Ethernet (RJ 21 or TELCO); 1 port Multimode OC12 ATM; 1 port Single Mode OC 12 ATM; 15 port 1000BASE T Gigabit Ethernet; 24 port 10BASE FL (MT RJ); Network Analysis Module; Flex Wan Module; 24 port FXS Analog Station Interface Module; 8 port Voice T1 or E1 Services Module; Voice Power Feature CardIntrusion Detection Module; Content Switching Module; Fabric Enabled Line Cards	Same as Catalyst 6503	Same as Catalyst 6503	Same as Catalyst 6503 plus: Switch Fabric Module 2
Backplane	Scalable to 256 Gbps	Scalable to 256 Gbps	Scalable to 256 Gbps	Scalable to 256 Gbps
Multilayer Performance	Scalable to 100+ Mpps	Scalable to 100+ Mpps	Scalable to 100+ Mpps	Scalable to 210 Mpps
VLAN Maximum	4000	4000	4000	4000
FEC/GEC	Up to 8 noncontiguous ports; supports multimode channeling.	Same as Catalyst 6503	Same as Catalyst 6503	Same as Catalyst 6503
Management Capabilities	CiscoWorks 2000, RMON, Enhanced Switched Port Analyzer (ESPAN), SNMP, Telnet, BOOTP, and Trivial File Transfer Protocol (TFTP)	Same as Catalyst 6503	Same as Catalyst 6503	Same as Catalyst 6503
Dimensions	7 x 17.37 x 21.75 in.	20.1 x 17.2 x 18.1 in.	25.2 x 17.2 x 18.1 in.	33.3 x 17.2 x 18.1 in.

Selected Part Numbers and Ordering Information[1]

Catalyst 6000 Family Chassis

WS-C6503	Catalyst 6500 3 Slot Chassis
WS-C6506	Catalyst 6506 Chassis
WS-C6509	Catalyst 6509 Chassis
WS-C6509-NEB	Catalyst 6509 Chassis for NEBS Environments
WS-C6513	Catalyst 6513 Chassis

Catalyst 6500 Series Power Supplies

PWR-950-AC=	Spare 950W AC P/S for Cisco 7603/Cat 6503
PWR-950-DC=	Spare 950W DC P/S for CISCO7603/Cat 6503
PEM-15A-AC=	Spare Pwr Entry Mod for CISCO7603/Cat 6503 (950W AC Pwr Sup)
PEM-DC/3=	Spare DC Power Entry Mod for CISCO7603/Cat 6503
WS-CAC-1000W=	Catalyst 6000 1000W AC Power Supply, Spare
WS-CAC-1300W=	Catalyst 6000 1300W AC Power Supply,Spare
WS-CDC-1300W=	Catalyst 6000 1300W DC Power Supply, Spare
WS-CAC-2500W=	Catalyst 6000 2500W AC Power Supply
WS-CAC-4000W-INT=	4000W AC PowerSupply, International (cableincluded)
WS-CAC-4000W-US=	4000Watt AC Power Supply for US (cable attached)

Catalyst 6000 Family Supervisor Engines and Switch Fabric Modules

WS-X6K-S1A-MSFC2=	Catalyst 6000 Supervisor Engine1-A, 2GE, plus MSFC-2 & PFC
WS-X6K-SUP1A-2GE=	Catalyst 6000 Supervisor Engine1A, Enhanced QoS, 2GE
WS-X6K-SUP1A-PFC=	Catalyst 6000 Supervisor Engine1-A, 2GE, plus PFC
WS-X6K-S2-PFC2=	Catalyst 6500 Supervisor Engine-2, 2GE, plus PFC-2
WS-X6K-S2-MSFC2=	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 & PFC-2
WS-X6K-S2U-MSFC2=	Cat6K Sup2 with 256MB DRAM on Sup2 and MSFC2
WS-SUP720=	Cat6500 CEF720 Sup Engine - Integrated Fabric, MSFC3
WS-C6500-SFM=	Catalyst 6500 Switch Fabric Module
WS-X6500-SFM2=	Catalyst 6500 Switch Fabric Module 2, Spare

Catalyst 6500 – 10 Gigabit Ethernet

WS-X6502-10GE=	Catalyst 6500 10 Gigabit Ethernet Base Module(Req OIM),Spare

Catalyst 6500 – Gigabit Ethernet

WS-X6148-GE-TX=	Cat6500 48-port 10/100/1000 GE Module, RJ45
WS-X6316-GE-TX=	Catalyst 6000 8-port GE, Enhanced QoS (Req. GBICs)
WS-X6408A-GBIC=	Catalyst 6000 8-port GE, Enhanced QoS (Req. GBICs)
WS-X6416-GBIC=	Catalyst 6000 16-port Gig-Ethernet Mod. (Req. GBICs)
WS-X6416-GE-MT=	Catalyst 6000, 16-port Gigabit EthernetModule, MT-RJ
WS-X6516-GBIC=	Catalyst 6500 16-port GigE Mod: fabric-enabled (Req. GBICs)
WS-X6516A-GBIC=	Catalyst 6500 16-port GigE Mod: fabric-enabled (Req. GBICs)
WS-X6516-GE-TX=	Catalyst 6500 16-port Gig/Copper Module,x-bar
WS-X6816-GBIC=	Catalyst 6500 16-port GigE mod, 2 fab I/F w/DF, (Req GBICs)

Catalyst 6500 – 10/100 Gigabit Ethernet

WS-X6024-10FL-MT=	Catalyst 6000 24-port 10BASE-FL MT-RJ Module
WS-X6148-RJ-21=	Catalyst 6500 48-Port 10/100 Upgradable to Voice, RJ-21
WS-X6148-RJ21V=	Catalyst 6500 48-port 10/100 Inline Power Module, RJ-21
WS-X6148-RJ-45=	Catalyst 6500 48-Port 10/100, Upgradable to Voice, RJ-45
WS-X6148-RJ45V=	Catalyst 6500 48-port 10/100 Inline Power, RJ-45
WS-X6324-100FX-MM=	Catalyst 6000 24-port 100FX, Enh QoS, MT-RJ, MMF
WS-X6324-100FX-SM=	Catalyst 6000 24-port 100FX, Enh QoS, MT-RJ, SMF
WS-X6348-RJ21V=	Catalyst 6000 48-port 10/100, Inline Power, RJ-21
WS-X6348-RJ-45=	Catalyst 6000 48-port 10/100, Enhanced QoS, RJ-45
WS-X6348-RJ-45V=	Catalyst 6000 48-port 10/100, Inline Power, RJ-45
WS-X6524-100FX-MM=	Catalyst 6500 24-port 100FX, MT-RJ, fabric-enabled
WS-X6548-RJ-21=	Catalyst 6500 48-port 10/100, RJ-21, fabric-enabled
WS-X6548-RJ-45=	Catalyst 6500 48-port 10/100, RJ-45, x-bar

Catalyst 6500 Services Modules

WS-SVC-CMM=	COMMUNICATION MEDIA MODULE
WS-SVC-CMM-6T1=	6-PORT T1 INTERFACE PORT ADAPTER
WS-SVC-CMM-6E1=	6-PORT E1 INTERFACE PORT ADAPTER
WS-SVC-CSG-1=	Content Services Gateway
WS-SVC-FWM-1-K9=	Firewall blade for Catalyst 6500
WS-SVC-IPSEC-1=	IPSec VPN Security Module for 6500 and 7600 series
WS-SVC-NAM-1=	Catalyst 6500 Network Analysis Module-1
WS-SVC-NAM-2=	Catalyst 6500 Network Analysis Module
WS-SVC-SSL-1-K9=	SSL Module for Catalyst 6500
WS-X6066-SLB-APC=	Catalyst 6500 Content Switching Module
WS-X6381-IDS=	Catalyst 6000 Intrusion Detection System Module
WS-X6608-E1=	Catalyst 6000 8-port Voice E1 and Services Module
WS-X6608-T1=	Catalyst 6000 8-port Voice T1 and Services Module
WS-X6624-FXS=	Catalyst 6000 24-port FXS Analog Station Interface Module

Catalyst 6500 FLEXWAN and OSM Modules

WS-X6101-OC12-MMF=	Catalyst 6000 1-port Multimode OC-12 ATM Module, Spare
WS-X6101-OC12-SMF=	Catalyst 6000 1-port Single-Mode OC-12 ATM Module, Spare
WS-X6182-2PA=	Catalyst 6000 Flex WAN Module (Supports 2 Port Adapters)
WS-X6516A-GBIC=	Catalyst 6500 16-port GigE Mod: fabric-enabled (Req. GBICs)

Catalyst 6500 Optics

WS-G5484=	1000BASE-SX Short Wavelength GBIC (Multimode only)
WS-G5486=	1000BASE-LX/LH long haul GBIC (single mode or multimode)
WS-G5487=	1000Base-ZX extended reach GBIC (single mode)
WS-G6483=	Cat 6500 10GBASE-ER Serial 1550nm extended reach OIM (spare)
WS-G6488=	Catalyst 6500 10GBASE-LR Serial 1310nm long haul OIM (spare)

Catalyst 6500 Bundles

WS-C6503-2GE	Cat6503 chassis w/ Sup1A-2GE (Requires Power Supply)
WS-C6503-PFC2	Cat6503 chassis w/ Sup2-PFC2 (Requires Power Supply)
WS-C6506-2GE	Cat6506 chassis w/ Sup1A-2GE (Requires Power Supply)
WS-C6506-PFC2	Cat6506 chassis w/ Sup2-PFC2 (Requires Power Supply)
WS-C6509-2GE	Cat6509 chassis w/ Sup1A-2GE (Requires Power Supply)
WS-C6509-PFC2	Cat6509 chassis w/ Sup2-PFC2 (Requires Power Supply)
WS-C6509-6816-16	Cat6509 w/S2-MSFC2,SFM2,WS-X6816-GBIC (Req Purch 2 2500W)
WS-C6509-6816-32	Cat6509 w/S2-MSFC2,SFM2,2xWS-X6816-GBIC (Req Purch 2 2500W)
WS-SVC-SSL-CSM-K9=	Catalyst 6500 SSL and CSM Bundle
WS-C6503-FWM-K9	Cisco Catalyst 6503 Firewall Security System
WS-C6506-FWM-K9	Cisco Catalyst 6506 Firewall Security System
WS-C6506-IPSEC-K9	Cisco Catalyst 6506 IPSec VPN System

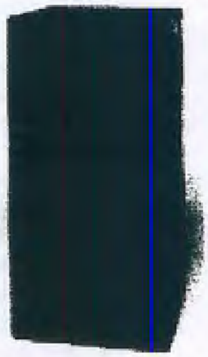
WS-C6503-IPSEC-K9	Cisco Catalyst 6503 IPsec VPN System
WS-C6506-IPSEC-K9	Cisco Catalyst 6506 IPSec VPN System
Catalyst 6000 Family Accessories	
WS-F6K-MSFC2=	Catalyst 6000 Multilayer Switch Feature Card (MSFQII, Spare
WS-F6K-VPWR=	Catalyst 6000 Voice Power Feature Card for WS-X6348-RJ-45
WS-F6K-DFC=	Distributed Forwarding Card
WS-C6X09-RACK=	Catalyst 6x00 Rack Mount Kit and Cable Organizer
WS-C6K-6SLOT-FAN=	Catalyst 6000, Fan Tray for 6-slot Systems
WS-C6X06-RACK=	Catalyst 6x06, Rack Mount Kit and Cable Organizer
Catalyst 6000 Family Software and Element Management Software (EMS)	
WS-C6513-EMS-LIC=	Catalyst 6513 RMON Agent License
WS-C6X09-EMS-LIC	Catalyst 6x09 RMON Agent License
WS-C6X06-EMS-LIC	Catalyst 6x06 RMON Agent License (also available for Cat6x09)
FRC6-MSM-IPX=	Catalyst 6000 MSM IPX Feature Set License, Spare
FR-IRC6=	Catalyst 6000 Family InterDomain Routing Feature License
S6MSFC2A-12102E=	Catalyst 6000 MSFC2 IOS Enterprise (also available in images with VIP, Desktop, IP/IPX, etc.)
SC6K-SUP2-6.1.1	Catalyst 6000 Supervisor 2 Flash Image, Rel 6.1(1)
SC6K-SUP2CV-6.1.1	Cat6K Supervisor 2 Flash Image w/CiscoView, Rel 6.1(1)
SC6K-SUP2K9-6.1.1	Catalyst 6000 Supervisor 2 Flash Image w/SSH, Rel 6.1(1)
SC6K-S2K9CV-6.1.1	Cat6K Sup 2 Flash Image w/CiscoView & w/SSH, Rel 6.1(1)
S6SUP22A-12105E	Catalyst 6000 Sup2/MSFC IOS Enterprise (also available in images with Desktop, IP, IP/IPX)
SC6K-SUP-5.4.4=	Catalyst 6000 Supervisor Flash Image, Release 5.4(4)
EMS-6500-025C-1.0=	6500 EMS 25 Chassis RTU License-6750 Per Chassis List
EMS-6500-100C-1.0=	6500 EMS 100 Chassis RTU License-6000 Per Chassis List
EMS-6500-250C-1.0=	6500 EMS 250 Chassis RTU License-5250 Per Chassis List
EMS-6500-500C-1.0=	6500 EMS 500 Chassis RTU License-4500 Per Chassis List
Catalyst 6000 Family Memory Options	
MEM-C6K-FLC16M=	Catalyst 6000, Supervisor PCMCIA 16MB Flash Memory Card
MEM-C6K-FLC24M=	Cat 6000 Sup PCMCIA Flash Memory Card, 24 MB Spare
MEM-MSFC-128MB=	Catalyst 6000 MSFC Mem, 128 MB DRAM Option
MEM-C6K-WAN-128M=	Catalyst 6000 WAN Module Memory, 128 MB
MEM-MSFC2-256MB=	MSFC2 256MB Memory Option (also available in 512 MB)
MEM-DFC-256MB=	Catalyst 6500 256 MB spare for DFC
MEM-DFC-512MB=	Catalyst 6500 512 MB option for DFC
MEM-S2-256MB=	256 MB DRAM spare for Sup2
Catalyst 6000 Family Packaged SMARTnet Maintenance 8x5xNBD	
CON-SNT-PKG12	Catalyst 6503 L2 Bundle SMARTnetMaintenance 8x5xNBD
CON-SNT-PKG14	Catalyst 6506 L2 Bundle SMARTnetMaintenance 8x5xNBD
CON-SNT-PKG15	Catalyst 6509 L2 Bundle SMARTnetMaintenance 8x5xNBD
CON-SNT-PKG16	Catalyst 6006 and 6506, Packaged SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG17	Catalyst 6009 and 6509, Packaged SMARTnet Maintenance 8x5xNBD

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Catalyst 6000 Family Web site: **http://www.cisco.com/go/6000**

Cisco Catalyst 8500 Multiservice Switch Routers



The Catalyst 8500 family multiservice switch routers integrate multiservice ATM switching with wire-speed multiprotocol routing for Gigabit Ethernet and Fast Ethernet into a single platform that also supports advanced Cisco IOS services for QoS and security. This family delivers enterprise MAN/WAN and Service Provider multiservice edge solutions with scalable performance, lower cost of ownership, and offer multiple interface options in a modular chassis. The Catalyst 8500 series consists of the modular Catalyst 8510 (10-Gbps, 5-slot) switch and the modular Catalyst 8540 (40-Gbps, 13-slot) switch. Both switches implement Cisco IOS Software to provide a variety of network services including reliability, security, management, and QoS with CiscoAssure policy networking.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 8540 and Catalyst 8510	• Integrated 10/100 FE, GE, and ATM • Flexible ATM interfaces (T1/E1, IMA, DS3/E3, OC-3, OC-12, and OC-48) • Frame relay and circuit emulation services • Wire-speed performance • Multiservice MAN/WAN applications • Multiservice Edge solutions • Voice, data, and video solutions • MPLS VPN

Key Features

- Ideal for integrated multiservice ATM switching with wire-speed multiprotocol routing for gigabit Ethernet (L3eATM or Layer 3 enabled ATM)
- Ideal for aggregating multiprotocol traffic from multiple wiring closets or from workgroup switches such as the Catalyst 5000 or distribution/server aggregation switches such as the Catalyst 6000 Family
- Provides nonblocking routing for IP, IPX, and IP multicast while also offering wire-speed Layer 2 switching for nonroutable protocols such as NetBIOS and DECnet local-area transport (LAT)
- Aggregate throughput of up to 24 million packets per second (pps) for non-blocking, wirespeed Layer 3 switching

Competitive Products

- Foundry: Big Iron
- Lucent: PSAX 1250 and 2300
- Marconi: ASX 1000, 1200, and 4000
- Alcatel: Omniswitch

Specifications

Feature	Catalyst 8510	Catalyst 8540
Modular Slots	5	13
Available Modules	See Part Numbers and Ordering information for a partial parts list	
Backplane	10 Gbps	40 Gbps
Throughput Performance	6 Mpps	24 Mpps
MAN / WAN	POS / ATM Uplink	POS / ATM Uplink
Dimensions (HxWxD)	10.5 x 17.2 x 18.14 in.	25.25 x 17.3 x 18.25 in.

Selected Part Numbers and Ordering Information[1]

Catalyst 8540—Common Equipment	
C8540MSR-SKIT-AC	C8540 MSR Starter Kit w/ Stratum 4Clock Module—AC Power(also available in DC Power)
C8545MSR-MRP4CLK=	C8540 MSR Multiservice Route Processor (spare)
C8545MSR-MRP3CLK=	C8540 MSR Route ProcessorStratum 3 (spare)
C8546MSR-MSP-FCL=	C8540 MSR Switch Processor with ATM FC (spare)
C8540CSR-SKIT-AC	Catalyst 8540 CSR Starter Kit with AC Power (also available in DC Power)
C8541CSR-RP=	Catalyst 8540 CSR Route Processor(spare)
C8542CSR-SP=	Catalyst 8540 CSR Switch Processor (spare)
C8540-CHAS13=	Catalyst 8540 - Chassis (spare)
C8540-PWR-AC=	C8540 Power Supply—AC (also available in DC Power)
Catalyst 8510—Common Equipment	
C8510MSR-SKIT-AC	Catalyst 8510 MSR Starter Kit with AC Power (alsoavailable as -DC for DC Power
C8515-MSRP=	C8510 Multiservice Switch Route Processor (spare)
C8510CSR-SKIT-AC	Catalyst 8510 CSR Starter Kit with AC Power (also available as -DC for DC Power)
C8510-SRP=	C8510 Layer 3 Switch Route Processor (spare)
C8510-CHAS5=	Catalyst 8510 - Chassis (spare)
C8510-PWR-AC=	C8510 power supply, AC (spare) (alsoavailable in DC power)
Catalyst 8500 Family—ATM Router Module Equipment	
C8540-ARM-64K=	C8540 ATM Router Module 64K (also available for 8510)
C8540-ARM2=	C8540 EnhancedATM Router Module (spare)
Catalyst 8500—Layer 3 Modules and ATM Interface Modules and Uplinks	
C85EGE-2X-16K=	C8540 2-port EnhancedGE 16K (also available in 64K and 256K)
C85GE-8X-64K=	C8540 8-port GE 64K
C85FE-16TACL-64K=	C8540 16-port 10/100 RJ-45 w/ACL 64K
C85FE-16FACL-64K=	C8540 16-port 100-FX MT-RJ w/ACL 64K
C8540-ACL=	C8540 ACL Daughter Card (also available for C8510/LS1010)
C85GE-1X-16K=	C8510/LS1010 1-port Gigabit Ethernet16K (also available in 64K)
C85FE-8T-64K=	C8510/LS1010 8-port 10/100 RJ-45 64K
C85FE-8F-64K=	C8510/LS1010 8-port 100-FX MT-RJ 64K
C85MS-1F4S-OC48SS=	C8540 1-port OC-48c/STM-16 SMF-IR+4-port OC-12 SMF
C85MS-1F4M-OC48SS=	C8540 1-port OC-48c/STM-16 SMF-IR+4-port OC-12 MMF
C85MS-4F-OC12SS=	C8540 4-port OC-12c/STM-4 SMF
C85MS-4F-OC12MM=	C8540 4-port OC-12c/STM-4 MMF
C85MS-16F-OC3MM=	C8540 16-port OC-3c/STM-1 MMF (spare)
C85MS-16F-OC3SM=	C8540 16-port OC-3c/STM-1 SMF-LR (spare)
Catalyst 8500—Port Adapter Modules	
C85MS-SCAM-2P=	C8540 SuperCAM for Port Adapter Modules (spare)
C8510TSCAM-2P=	CS8510/LS1010 Traffic Shaping Carrer Access Modules (spare)
WATM-CAM-2P=	C8510 / LS1010 Carrier Modules (spare)
WAI-T1C-4RJ48=	4 Port T1 (circuit emulation) RJ-48 PAM (also available in El andin E1 BNC)
C85MS-4E1-FRRJ48=	C8500 4-port E1 Frame-Relay/FUNI PAM (spare)
WAI-OC3-4MM=	4 Port OC-3c/STM-1 MMF PAM (also available in SMF-IR & SMF-LR)
WAI-OC3-1S3M=	OC-3c/STM-1 Mix PAM, 1-port SMF-IR + 3-port MMF (spare)
WAI-OC12-1MM=	1 Port OC-12c/STM-4c MMF PAM (also available in SMF-IR and SMF-LR)
WAI-T3-4BNC=	4 Port DS-3 PAM (spare and in E3 BNC)
C85MS-8T1-IMA=	C8500MSR/LS1010 8-port TI IMA PAM (also available in E1 120 ohm)
WAI-T1-4RJ48=	4 Port T1 (ATM) RJ-48 PAM (spare also available in E1 and E1 BNC E1)
Catalyst 8500 Software Feature License Options	
FR-8510-TAGSW=	C8510 Tag Switching upgrade license (also available with HPNNI and HPNNI + Tag Switching)
FR-8540MSR-HPNNI=	Cat 8540MSR—Hierarchical PNNI License (also available with Tag Switching)

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Catalyst 8500 series Web site: **http://www.cisco.com/go/8500**

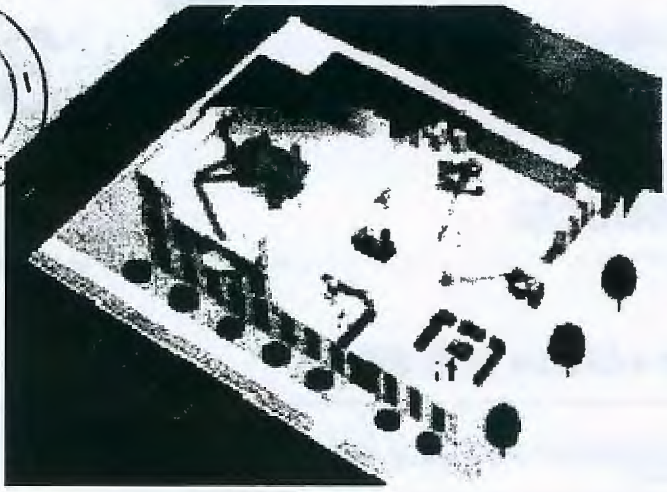
CHAPTER 3

Wireless LAN Products

Wireless LAN Products at a Glance (IEEE 802.11b)

Product	Features	Page
Cisco Aironet 1200 Series Access Points	• Offers investment protection and a smooth migration path to future technologies througha dual band radio design • Delivers an enterprise class security solution with the IEEE 802.11x-based Cisco Wireless Security Suite • Industry-leading security, network management, throughput and software feature set • Support for both line power over Ethernet and localpower	3-2
Cisco Aironet 1100 Series Access Point	• Single 802.11b radio, upgradableto 802.11g • Provides end-to-endsolution support for Intelligent NetworkServices • Delivers an enterprise class security solution with the IEEE 802.11x-based Cisco Wireless Security Suite • Support for both line power over Ethernet and local power • Cost effective, yet feature-rich	3-5
Cisco Aironet 5 GHz 54 Mbps Wireless LAN Client Adapter	• IEEE 802.11a-compliant CardBus adapterthat operatesin the UNII-1 and UNII-2 bands • Complementsthe Cisco Aironet 1200 Series 802.11a Access Point, providing a solution that combinesperformanceand mobilitywith the security and manageability that enterprises require	3-6
Cisco Aironet 350 Series Client Adapters	• Superior range and throughput • Secure networkcommunications • World mode for internationalroaming • PCMCIA card and PCI form factors • IEEE 802.11b	3-8
Cisco Aironet 350 Series Workgroup Bridge	• Driverless installation of up to eight Ethernet-enabled devices • Optimum wireless performance and range • Standards-based centralized security • IEEE 802.11b	3-10
Cisco Aironet 350 Series Wireless Bridge	• High-speed, high-power radios, delivering building-to-building links of up to 25 miles (40.2 km) • A metal casefor durability and plenum rating • Supports both pointto-point and point-to-multipoint configurations • Broad range of support antennas • Simplified installation, improved performance, and upgradeablefirmware, ensuring investment protection • IEEE 802.11b	3-12
Cisco Aironet Antennas and Accessories	• A wide array of options • FCC-approved directionaland omni-directional antennas • Low-loss cable, mounting hardware, and other accessories available	3-14
CiscoWorks Wireless LAN Solution Engine	A hardware-based wireless LAN managementsolution that providestemplate-based configuration with user-defined groupsto effectively manage a large numberof accesspoints and bridges. • Monitors LEAP authentication servers • Enhancessecurity management through misconfiguration detection on acces points and bridges	9-23

Sample Wireless LAN Solution Overview—In-Building or Site-to-Site



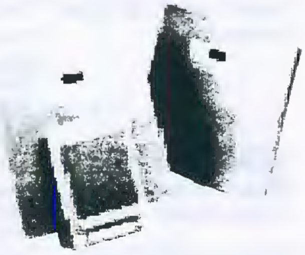
Enterprise, Small/Medium Business Applications

Service common areas for mobile workers
Support employees working in multiple offices
Cost effective, quick network deployment for temporary or leased offices

Sample Vertical Markets

Healthcare, retail, government
Public Access
Multiple Tenant/Dwelling Units
Airports, Hotels, Convention Centers
Education: K-12 and Universities

Cisco Aironet 1200 Series Access Points



The Cisco Aironet 1200 Series Access Point sets the enterprise standard for next-generation high performance secure, manageable, and reliable wireless local-area networks (WLANs) while also providing investment protection because of its upgrade capability and compatibility with current standards. The modular design of the Cisco Aironet 1200 supports IEEE 802.11a and 802.11b technologies in both single-and dual-mode operation. You can configure the Cisco Aironet 1200 to meet customer-specific requirements at the time of purchase and then reconfigure and upgrade the product in the field as these requirements evolve.

The Cisco Aironet 1200 Series protects current and future network infrastructure investments. Compliant with IEEE 802.11a and 802.11b standards, The 802.11a radio supports data rates of up to 54 Mbps and eight non-overlapping channels that offer high performance as well as maximum capacity and scalability. The 802.11b radio provides data rates up to 11 Mbps and three non-overlapping channels to support widely deployed 802.11b clients. The Mini-PCI form factor of the 802.11b radio allows for upgrade to higher-speed 2.4 GHz technologies such as the draft IEEE 802.11g standard.The Cisco Aironet 1200 Series extends end-to-end intelligent networking to the wireless access point with support for enterprise-class virtual LANs (VLANs) and quality of service (QoS). An ideal choice for enterprise installations, the Cisco Aironet 1200 Series can manage up to 16 VLANs, which allows customers to differentiate LAN policies and services, such as security and QoS, for different users. Traffic to and from wireless clients with varying security capabilities can be segregated into VLANs with varying security policies.

Wireless LAN security is a primary concern. The Cisco Aironet 1200 Series secures the enterprise network with a scalable and manageable system featuring the award-winning Cisco Wireless Security Suite. Based on the 802.11x standard for port-based network access, the Cisco Wireless Security Suite takes advantage of the Extensible Authentication Protocol (EAP) framework for user-based authentication.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 1200 Series Access Point	• IT Professionals or business executives want mobility within the enterprise to increase productivity, as an addition or alternative to wired networks. • Business owners or IT directors need flexibility for frequent LAN wiring changes, either throughout the site or in selected areas • Any company whose site is not conducive to LAN wiring because of building or budget limitations, such as older buildings, leased space or temporary sites.

Key Features

- Offers investment protection because of its upgrade capability and compatibility with current standards
- Delivers an enterprise class security solution with the IEEE 802.11x-based Cisco Wireless Security Suite
- Industry-leading security, network management, and software feature set
- Support for both inline power over Ethernet or local power
- Simultaneous support for both IEEE 802.11b and IEEE 802.11a

Specifications

Feature	Cisco Aironet 1200 Series Access Points with 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Data Rates Supported	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, and 11 Mbps	Same as 802.11a and 802.11b combined
Uplink	Autosensing 802.3 10/100BaseT Ethernet	Autosensing 802.3 10/100BaseT Ethernet	Same as 802.11a and 802.11b combined
Form Factor	CardBus (32-bit)	Mini-PCI	Same as 802.11a and 802.11b combined
Frequency Band	5.15 to 5.35 GHz (FCC UNII 1 and UNII 2), 5.15 to 5.25 GHz (TELEC),5.15 to 5.25 GHz (Singapore),5.25 to 5.35 GHz (Taiwan)	2.412 to 2.462 GHz (FCC),2.412 to 2.472 GHz (ETSI),2.412 to 2.484 GHz (TELEC),2.412 to 2.462 GHz (MII),2.422 to 2.452 GHz (Israel)	Same as 802.11a and 802.11b combined
Wireless Medium	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS)	Same as 802.11a and 802.11b combined
Modulation	(OFDM subcarrier);BPSK @ 6 and 9 Mbps; QPSK @ 12 and 18 Mbps; 16-QAM @ 24 and 36 Mbps;64-QAM @ 48 and 54 Mbps	DBPSK @1 Mbps; DQPSK @ 2 Mbps; CCK @ 5.5 and 11 Mbps	Same as 802.11a and 802.11b combined
Operating Channels	FCC: 8;TELEC (Japan): 4; Singapore: 4; Taiwan: 4	ETSI: 13; Israel: 7; North America: 11; TELEC (Japan): 14; MII: 11	Same as 802.11a and 802.11b combined
Nonoverlapping Channels	Eight (FCC only); Four (Japan, Singapore, Taiwan)	Three	Eleven
Available Transmit Power Settings[1]	40 mW (16 dBm);20 mW (13 dBm);10 mW (10 dBm);5 mW (7 dBm); Maximum power setting will vary according to individual country regulations.	100 Mw (20 dBm); 5 Mw (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm); Maximum power setting will vary according to individual country regulations	Same as 802.11a and 802.11b combined
Range (typical @ maximum power setting, 2.2 dBi gain diversity dipole antenna)	Omni directional Antenna: Indoor:60 ft (18m)@ 54 Mbps, 130 ft (40m) @ 18 Mbps, 170 ft (52m) @ 6 Mbps; Outdoor: 100 ft (30m) @ 54 Mbps, 600 ft (183m) @ 18 Mbps, 1000 (304m) ft @ 6 Mbps; Patch Antenna: Indoor: 70 ft (21m) @ 54 Mbps, 150 ft (45m) @ 18 Mbps, 200 ft (61m) @ 6 Mbps; Outdoor: 120 ft (36m) @ 54 Mbps, 700 ft (213m) @ 18 Mbps; 1200 ft (355m) @ 6 Mbps	IIndoor:130 ft (40m) @ 11 Mbps; 350 ft (107m) @ 1 Mbps Outdoor: 800 ft (244m) @ 11 Mbps; 2000 ft (610m) @ 1Mbps	Same as 802.11a and 802.11b combined
SMTP Compliance	MIB I and MIB II	MIB I and MIB II	MIB I and MIB II
Antenna	Integrated 6 dBi diversity patch (55 degree horizontal, 55 degree vertical beamwidths, 5 dBi diversity omnidirectional with 360 degree horizontal and 40 degree vertical beamwidths	Two RP-TNC connectors (antennas optional, none supplied with unit)	5 GHz: Integrated6 dBi diversity patch (55 degree horizontal, 55 degree vertical beamwidths, 5 dBi diversity omnidirectional with 360 degree horizontal and 40 vertical beamwidths; 2.4 GHz: Two RP-TNC connectors (antennas optional, none supplied with unit)

Feature	Cisco Aironet 1200 Series Access Points with 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Security architecture client authentication	Cisco Wireless Security Suite including: Authentication: 802.11x support including LEAP, PEAP, EAP-TLS, EAP-TTLS, and EAP-SIM to yeld mutual authentication and dynamic, per-user, per-session WEP keys; MAC address and by standard 802.11 authentication mechanisms Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; Pre-standard TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation	Cisco Wireless Security Suite including: Authentication: 802.11x support including LEAP, PEAP, EAP-TLS, EAP-TTLS, and EAP-SIM to yeld mutual authentication and dynamic, per-user, per-session WEP keys; MAC address and by standard 802.11 authentication mechanisms Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; Pre-standard TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation	Same as 802.11a and 802.11b combined
Software Image Network and Inventory support	CiscoWorks RME[2], CiscoWorks SWIM[3]	CiscoWorks RME[2], CiscoWorks SWIM[3]	CiscoWorks RME[2], CiscoWorks SWIM[3]
Remote configuration support	BOOTP, DHCP, Telnet, HTTP, FTP, TFTP, and SNMP	Telnet, HTTP, FTP, TFTP, and SNMP	Telnet, HTTP, FTP, TFTP,and SNMP
Local configuration	Direct consoled port (RJ-45 interface)	Direct consoled port (RJ-45 interface)	Direct consoled port (RJ-45 interface)
Environmental	-4° to 122°F (-20° to 50°C), 10 to 90% humidity (noncondensing)	-4° to 131°F (-20° to 55°C), 10 to 90% humidity (noncondensing)	-4° to 122°F (-20° to 50°C), 10 to 90% humidity (noncondensing)
Input Power Requirements	90 to 240 VAC +/- 10% (power supply);48 VDC +/- 10%(device)	90 to 240 VAC +/- 10% (power supply);48 VDC +/- 10%(device)	90 to 240 VAC +/- 10% (power supply);48 VDC +/- 10%(device)
Power Draw	8 watts, RMS	6 watts, RMS	11 watts, RMS
Warranty	One year	One year	One year

1. Management Information Base
2. CiscoWorks Resource Manager Essentials
3. Software Image Manager

Selected Part Numbers and Ordering Information[1]

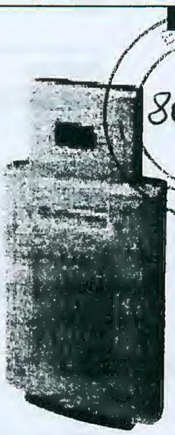
1200 Series Access Points	
AIR-AP1200	AP Platform, Cardbus and MPCI Slots (no radio), Enet Uplink
AIR-AP1220B-A-K9	802.11b AP w/Avail CBus Slot, FCC Cnfg
AIR-AP1220B-E-K9	802.11b AP w/Avail CBus Slot, ETSI Cnfg
AIR-AP1220A-J-K9	802.11a AP w/Avail MPCI Slot, Enet Uplink, TELEC Cnfg
AIR-AP1220B-J-K9	802.11b AP w/Avail CBus Slot, Japan Cnfg
1230 Series Access Points	
AIR-AP1210	IOS based AP Platform, Cardbus and MPCI Slots (no radio), Enet Uplink
AIR-AP1230B-A-K9	IOS based 802.11b AP w/Avail CBus Slot, FCC Cnfg
AIR-AP1230B-E-K9	IOS based 802.11b AP w/Avail CBus Slot, ETSI Cnfg
AIR-AP1230A-J-K9	IOS based 802.11a AP w/Avail MPCI Slot, Enet Uplink, TELEC Cnfg
AIR-AP1230B-J-K9 I	OS based 802.11b AP w/Avail CBus Slot, Japan Cnfg

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the Distribution Product Reference Guide at: http://www.cisco.com/dprg (limited country availability)

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 1100 Series Access Points



The Cisco Aironet® 1100 Series Access Point provides a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals.

Taking advantage of the Cisco Wireless Security Suite for the strongest enterprise security available and of Cisco IOS® Software for ease-of-use and familiarity, the Cisco Aironet 1100 Series Access Point delivers manageability, performance, investment protection, and scalability in a cost-effective package with a low total cost of ownership. The Cisco Aironet 1100 Series features a single, upgradable 802.11b radio, integrated diversity dipole antennas, and an innovative mounting system for easy installation in a variety of locations and orientations.

The first access point based on Cisco IOS Software, the Cisco Aironet 1100 Series extends end-to-end intelligent networking to the wireless access point. Cisco command-line interface (CLI) allows customers to quickly and consistently implement extended capabilities available in Cisco IOS Software. Customers can manage and standardize their networks using tools they have developed internally for their Cisco routers and switches.

Enterprise-class features including virtual LANs (VLANs), quality of service (QoS), and proxy mobile Internet Protocol (IP) make the Cisco Aironet 1100 Series ideal for enterprise installations. The Cisco Aironet 1100 Series also supports standard Cisco Aironet features such as hot-standby and load balancing, allowing enterprises to implement intelligent, reliable network services.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 1100 Series Access Point	• A cost-effective and upgradable WIAN solution that combines the mobility and flexibility of a WLAN solution with the enterprise-class features required by a business LAN. Want an off the shelf WLAN solution that does not require simultaneous dual band operation, or the additional range offered by high-gain antennas.

Key Features

- Single 802.11b radio, upgradable to 802.11g
- Provides end-to-end solution support for Intelligent Network Services
- Variety of mounting options
- Cost effective, yet feature-rich

Specifications

Feature	Cisco Aironet 1100 Series Access Points
Data Rates Supported	1, 2, 5.5, 11 Mbps
Network standard	IEEE 802.11b
Uplink	Autosensing 802.3 10/100BaseT Ethernet
Frequency Band	2.412 to 2.462 GHz (FCC); 2.412 to 2.472 GHz (ETSI); 2.422 to 2.452 GHz (Israel); 2.412 to 2.484 GHz (TELEC)
Network architecture type	Infrastructure,star topology
Wireless Medium	Direct Sequence Spread Spectum (DSSS)
Modulation	DBPSK @ 1 Mbps; DQPSK @ 2 Mbps; CCK @ 5.5 and 11 Mbps
Operating Channels	ETSI: 13; Israel: 7; Americas: 11; TELEC (Japan): 14
Nonoverlapping Channels	Three
Receive sensitivity	1 Mbps: -94 dBm; 2 Mbps: -91 dBm; 5.5 Mbps: -89 dBm;11 Mbps: -85 dBm

Feature	Cisco Aironet 1100 Series Access Points
Available Transmit Power Settings[1]	100 mW (20 dBm); 50 mW (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm) Maximum power setting will vary according to individual country regulations
Range (typical @ maximum power setting, 2.2 dBi gain diversity dipole antenna)	Indoor: 150 ft (45 m) @ 11 Mbps;; 400 ft (122 m) @ 1 MbpsOutdoor: 800 ft (244 m) @ 11 Mbps; 2000 ft (610 m) @ 1 Mbps
SMTP Compliance	MIB I and MIB II
Antenna	Integrated 2.2dBi diversity dipole antennas
Security architecture client authentication	Cisco Wireless Security Suite includingAuthentication: 802.11x support including LEAP, PEAP, EAP-TLS, EAP-TTLS and EAP-SIM to yield mutual authentication and dynamic, per-user, per-session WEP keys; MAC address and by standard 802.11 authentication mechanisms Encryption: Support forstatic and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; Pre-standard TKIP WEP enhancements:key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation
Software Image Network and Inventory support	CiscoWorks CiscoView, Resource Manager Essentials, and Campus Manager
Remote configuration support	BOOTP, DHCP, Telnet, HTTP, FTP, TFTP, and SNMP
Dimensions	4.1 in. (10.4 cm) wide; 8.1 in. (20.5 cm) high; 1.5 in. (3.8 cm) deep
Weight	10.5 oz. (297 g)
Environmental	;32° to 104° F (0° to 40° C); 10-90% humidity (noncondensing)
System Memory	16 MB RAM; 8 MB Flash
Input Power Requirements	100 to 240 VAC 50 to 60Hz (power supply); 33 to 57 VDC (device)
Power Draw	4.9 watts, RMS
Warranty	One year

[1] Management Information Base

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 5 GHz 54 Mbps Wireless Client Adapter

The Cisco Aironet® 5 GHz 54 Mbps Wireless LAN client adapter is an Institute of Electrical and Electronic Engineers (IEEE) 802.11a-compliant CardBus adapter that operates in the UNII-1 and UNII-2 bands. The client adapter complements the Cisco Aironet 1200 Series 802.11a Access Point, providing a solution that combines performance and mobility with the security and manageability that enterprises require.

Wireless LAN client adapters can increase productivity by enabling mobile users to have network and Internet access anywhere within a building that is equipped with a wireless network infrastructure. Wireless client adapters connect a variety of devices to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with access points. With this client adapter, you can quickly add new employees to a network, support temporary workgroups, or enable Internet access in conference rooms or other meeting spaces. And the Cisco Aironet client solution is easy to use, making the benefits of wireless mobility completely transparent.

With Cisco, you can confidently deploy a wireless solution that provides robust enterprise-class security. All Cisco Aironet products feature the award-winning Cisco Wireless Security Suite, which is based on the IEEE 802.11x standard for port-based network access.

The Cisco Wireless Security Suite takes advantage of the Extensible Authentication Protocol (EAP) framework for user-based authentication. It supports a variety of 802.11x authentication types including EAP Cisco Wireless (LEAP) and EAP-Transport Layer Security (EAP-TLS).

The Cisco Aironet Client Utility (ACU), with an intuitive graphical user interface, provides an easy way to configure, monitor, and manage the Cisco Aironet 5 GHz Wireless LAN Client Adapter. The ACU includes site-survey tools that present easy-to-understand detailed graphical information to assist in the placement of access points. Profile Manager allows you to create specific profile settings for various environments, such as the office or home, making it simple for telecommuters and business travelers to move from one environment to another.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 5 GHz 54Mbps Wireless LAN Client Adapters	• Industry leading security: IEEE802.11x support,including LEAP and EAP-TLS,for mutual authentication and dynamic per-user, per session WEP keys • Multiple transmit power settings (20 mW/(13 dBm), 10 mW/(10 dBm), and 5 mW (7 dBm) • End-to-end Cisco branded solution

Key Features

- IEEE 802.11a-compliant CardBus adapter that operates in the UNII-1 and UNII-2 bands
- Complements the Cisco Aironet 1200 Series 802.11a Access Point, providing a solution that combines performance and mobility with the security and manageability that enterprises require

Specifications

Feature	Cisco Aironet 5 GHz 54 Mbps Wireless Client Adapter
Form Factor	CardBus Type II
Interface	32-bit CardBus (PCI)
Operational voltage	3.3 V (+/- 0.33 V)
LED	Status (green) and Activity (amber)
Data Rates Supported	6, 9, 12, 18, 24, 36, 48, 54 Mbps (configurable as fixed or auto selecting to extend range)
Network Standard	IEEE 802.11a
Frequency Band	5.15 to 5.35 GHz (FCC UNII 1 and UNII 2) 5.15 to 5.25 GHz (TELEC); 5.15 to 5.25 GHz (Singapore); 525 to 5.35 GHz (Taiwan)
Network architecture type	Infrastructure,star topology
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Wireless Medium	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation	(OFDM sub-carrier); BPSK @ 6 and 9 Mbps; QPSK @ 12 and 18 Mbps; 16-QAM @ 24 and 36 Mbps; 64-QAM @ 48 and 54 Mbps
Operating Channels	FCC: 8 channels (UNII-1 4 channels and UNII-2 4 channels);4 channels for Japan, Singapore, and Taiwan
Available Transmit Power Settings[1]	20 mW (13 dBm);10 mW (10 dBm); 5 mW (7 dBm) Maximum power setting will vary according to individual country regulations.
Current steady state (typical)	¡Transmit: 520 mA; Receive: 580 mA; Sleep: 20 mA
Range	Omni directional Antenna: Indoor:60 ft (18m)@ 54 Mbps, 130 ft (40m) @ 18 Mbps, 170 ft (52m) @ 6 Mbps Outdoor: 100 ft (30m) @ 54 Mbps, 600 ft (183m) @ 18 Mbps, 1000 (304m) @ 6 Mbps Patch Antenna:Indoor: 70 ft (21m) @ 54 Mbps, 150 ft (45m) @ 18 Mbps, 200 ft (61m) @ 6 Mbps Outdoor: 120 ft (36m) @ 54 Mbps, 700 ft (213m) @ 18 Mbps, 1200 ft (355m) @ 6 Mbps
Power Management	3 levels of power consumption available, including: CAM (Constantly Awake Mode), Fast PSP (Power Save Mode), Max PSP (Maximum Power Savings)
Antenna	Integrated 5dBigain patch antenna

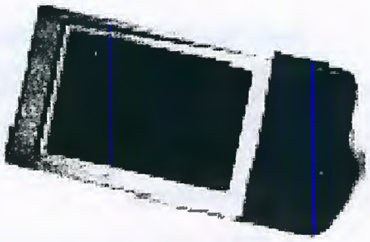
Feature	Cisco Aironet 5 GHz 54 Mbps Wireless Client Adapter
Security architecture client authentication	Cisco Wireless Security Suite including: Authentication:802.11x support for LEAP and EAP-TLS to yield mutual authentication and dynamic, per-user, per-session WEP keys; MAC address and by standard 802.11 authentication mechanisms Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; Pre-standard TKIP WEP enhancements:key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation
Drivers	Windows, 98/98SE, Windows ME, Windows 2000 and Windows XP
Environmental	-30° to 70°C; 95% humidity (noncondensing)
Warranty	One year

1. Management Information Base

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 350 Series Client Adapters



Wireless client adapters are the key to adding mobility and flexibility to an enterprise—increasing productivity by enabling users to have network and Internet access anywhere within a building without the limitation of wires. The Cisco Aironet 350 Series 802.11b Client Adapters are a complement to Aironet 350 Series infrastructure devices, providing an enterprise-ready solution that combines mobility with the performance, security, and manageability that people have come to expect from Cisco. Wireless client adapters connect a variety of devices to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with Access Points. Available in PC Card (PCMCIA) and Peripheral Component Interconnect (PCI) form factors, Cisco Aironet 350 Series Client Adapters quickly connect desktop and mobile computing devices wirelessly to all network resources. With this product, you can instantly add new employees to the network, support temporary workgroups, or enable Internet access in conference rooms or other meeting spaces.

Cisco Aironet 350 Series Client Adapters deliver superior range, reliability, and performance for business users needing information access anytime, anywhere. Combined with Cisco Aironet unique security services, this product ensures that business-critical information is secure. Most importantly, the Cisco client solution is easy to use, making the benefits of wireless mobility completely transparent.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 350 Series Client Adapters	• IT Professionals or business executives want mobility within the enterprise to increase productivity, as an addition or alternative to wired networks. • Business owners or IT directors need flexibility for frequent LAN wiring changes, either throughout the site or in selected areas • Any company whose site is not conducive to LAN wiring because of building or budget limitations, such as older buildings, leased space or temporary sites.

Key Features

- Superior range and throughput for IEEE 802.11b networks
- Secure network communications
- World mode for international roaming
- Full-featured utilities for easy configuration and management
- Compliance with the IEEE 802.11b high-rate standard
- Support for all popular operating systems

Specifications

Feature	Cisco Aironet 350 Series Client Adapters
Data Rates Supported	1, 2, 5.5, and 11 Mbps
Network Standard	IEEE 802.11b
System Interface	AIR-PCM35x: PC Card (PCMCIA) Type II AIR-PCI 35x: peripheral component interconnect (PCI) Bus
Frequency Band	2.4 to 2.4897 GHz
Network Architecture Types	Infrastructure andad hoc
Wireless Medium	Direct Sequence Spread Spectum (DSSS)
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	DBPSK @1 Mbps; DQPSK @ 2 Mbps; CCK @ 5.5 and 11 Mbps
Operating Channels	North America: 11; ETSI: 13; Japan: 14
Nonoverlapping Channels	Three
Receive Sensitivity	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5.5 Mbps: -89 dBm 11 Mbps: -85 dBm
Delay Spread	1 Mbps: 500 ns; 2 Mbps: 400 ns; 5.5 Mbps: 300 ns; 11 Mbps: 140 ns
Available Transmit Power Settings[1]	100 mW (20 dBm); 50 mW (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm)
Range (typical)	Indoor: 130 ft (40 m) @ 11 Mbps; 350 ft (107 m) @ 1 Mbps Outdoor: 800 ft (244 m) @ 11 Mbps; 2000 ft (610 m) @ 1 Mbps
Compliance	Operates license free under FCC Part 15 and complies as a Class B device; complies with DOC regulations; complies with ETS 300.328, FTZ 2100, and MPT 1349 standards
Operating Systems Supported	Windows 95, 98, NT 4.0, 2000, ME, XP, CE 2.11, CE 3.0, Mac OS 9.x, and Linux
Antenna	AIR-PCM35x: Integrated diversity dipoles AIR-LMC35x: Two MMCX connectors (antennas optional, none supplied with unit) AIR-PCI35x: External, removable 2.2 dBi Dipole with RP-TNC Connector
Encryption Key Length	128-bit
Authentication Type	EAP-Cisco Wireless LEAP
Status Indicators	Link Status and Link Activity
Dimensions (W x D x H)	AIR-PCM35x: 2.13 in. (5.4 cm) x 4.37 in. (11.1 cm) x 0.1 in. (0.3 cm) AIR-LMC35x: 2.13 in. (5.4 cm) x 3.31 in. (8.4 cm) x 0.1 in. (0.3 cm) AIR-PCI35x: 6.6 in. (16.8 cm) x 3.9 in. (9.8 cm) x .5 in. (1.3 cm)
Weight	AIR-PCM35x: 1.6 oz (45g) AIR-LMC35x: 1.4 oz (40g) AIR-PCI35x: 4.4 oz (125g)
Environmental	AIR-PCM35x and AIR-LMC35x: -22° to 158° F (-30° to 70° C) AIR-PCI35x: 32° to 131° F (0° to 55° C) 10 to 90% (noncondensing)
Input Power Requirements	+5 VDC =/- 5%
Typical Power Consumption (at 100 mW transmit power setting)	Transmit: 450 mA; Receive: 270 mA; Sleep mode: 15 mA

1. Maximum power setting will vary according to individual country regulations.

Selected Part Numbers and Ordering Information[1]

Cisco Aironet 350 Series Client Adapters

AIR-PCM352	350 Series PC Card with Diversity Antennas & 128-bit WEP
AIR-PCI352	350 Series PCI Card with 2.2 dBi Dipole Antenna & 128-bit WEP

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability)

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 350 Series Workgroup Bridge

Designed to meet the needs of remote workgroups, satellite offices, and mobile users, the Cisco Aironet 350 Series Workgroup Bridge brings the freedom and flexibility of wireless connectivity to any Ethernet-enabled device. The 802.11b workgroup bridge quickly connects up to eight Ethernet-enabled laptops or other portable computers to a wireless LAN (WLAN), providing a link from these devices to any Cisco Aironet Access Point (AP) or Wireless Bridge (line-of-sight).

Any Ethernet-ready device, including printers, copiers, PCs, point-of-sale devices, or monitoring equipment, can be placed directly at the point of work using the workgroup bridge—without the expense or delay of cabling. For temporary classrooms or temporary office space, the workgroup bridge provides flexible, easy network access for up to eight devices through the use of a standard eight-port Ethernet hub. Equipment can be easily moved as workgroups change in number or location, lowering facilities costs.

The Cisco Aironet 350 Series Workgroup Bridge supports Wired Equivalent Privacy (WEP) security architecture and provides up to 128-bit encryption. The Cisco Aironet security architecture is based upon an IEEE 802.11x standard utilizing the Extensible Authentication Protocol (EAP), an open standard that enables wireless manufacturers and RADIUS server vendors to independently develop interoperable hardware and software. For authentication of devices attached to the workgroup, a username and password may be stored in the workgroup bridge in either static or dynamic memory. When authenticated, the workgroup bridge receives a single-session, single-user encryption key from the Remote Access Dial-In User Service (RADIUS) server via the associated AP. With this centralized and standards-based architecture, wireless security scales to meet the requirements of any enterprise.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 350 Series Workgroup Bridge	• Connectivityto a networkfor remote workgroupslocatedin an area that may be difficult or not practical for wiring. • Supports upto eight Ethernet-baseddevices (with use of Ethernet hub)

Key Features

- Driverless installation of up to eight Ethernet-enabled devices
- Optimum wireless performance and range
- Standards-based centralized security
- Two versions for a range of application requirements
- Full-featured utilities and robust management

Specifications

Feature	Cisco Aironet 350 Series Workgroup Bridge
Data Rates Supported	1, 2, 5.5, and 11 Mbps
Client Interface	10BaseT Ethemet
Clients Supported	Direct: One Via hub: Eight
Network Architecture Types	Infrastructure(via Cisco Aironet Access Point or Bridge)
Frequency Band	2.4 to 2.4897 GHz
Wireless Medium	Direct Sequence Spread Spectum (DSSS)
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	DBPSK @1 Mbps; DQPSK @ 2 Mbps; CCK @ 5.5 and 11 Mbps
Operating Channels	North America: 11; ETSI: 13; Japan: 14
Nonoverlapping Channels	Three
Receive Sensitivity	1 Mbps: -94 dBm; 2 Mbps: -91 dBm; 5.5 Mbps: -89 dBm; 11 Mbps: -85 dBm
Delay Spread	1 Mbps: 500 ns; 2 Mbps: 400 ns; 5.5 Mbps: 300 ns; 11 Mbps: 140 ns
Available Transmit Power Settings[1]	100 mW (20 dBm); 50 mW (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm)
Range (typical)	Indoor: 130 ft (40 m) @ 11 Mbps; 350 ft (107 m) @ 1 Mbps Outdoor: 800 ft (244 m) @ 11 Mbps; 2000 ft (610 m) @ 1 Mbps
Compliance	Operates license free under FCC Part 15 and complies as a Class B device; complies with DOC regulations; complies with EN 300.328 standards
SNMP Compliance	MIB I and MIB II
Antenna	AIR-WGB352C: One nonremovable 2.2-dBi dipole AIR-WGB352R: Two RP-TNC connectors(antennas optional, none supplied with unit)
Encryption Key Length	AIR-WGB352x: 128-bit
Remote Configuration Support	Telnet, HTTP, FTP, TFTP, and SNMP
Dimensions (W x D x H)	6.30 in. (16 cm) x 4.72 in. (12 cm) x 1.45 in. (3.7 cm)
Weight	12.3 oz (350g)
Environmental	Temperature: 32° to 122° F (0° to 50° C); 10 to 90% (Noncondensing)
Input Power Requirements	North American: 120 VAC @ 60 Hz; Universal: 90 to 264 VAC @ 47 to 63 Hz

[1] Maximum power setting will vary according to individual country regulations.

Selected Part Numbers and Ordering Information[1]

Cisco Aironet 350 Series Workgroup Bridge

AIR-WGB352C	350 Series Workgroup Bridge with Captured Antenna & 128-bit WEP
AIR-WGB352R	350 Series Workgroup Bridge with Dual RP-TNC & 128-bit WEP

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability)

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 350 Series Wireless Bridge

The Cisco Aironet 350 Series Wireless Bridge enables high-speed long-range outdoor links between buildings and is ideal for installations subject to plenum rating and harsh environments. It is designed to meet the requirements of even the most challenging applications. The 802.11b wireless bridge delivers high data rates and superior throughput for data-intensive, line-of-sight applications. The bridges connect hard-to-wire sites, noncontiguous floors, satellite offices, school or corporate campus settings, temporary networks, and warehouses. They can be configured for point-to-point or point-to-multipoint applications and allow multiple sites to share a single, high-speed connection to the Internet. For functional flexibility, the wireless bridge may also be configured as an access point.

The Cisco Aironet 350 Series Wireless Bridge features an extended operating temperature range of -20° to 55° C, allowing for placement outdoors in a NEMA enclosure or in harsh indoor environments such as warehouses and factories. With a durable metal case, the Cisco Aironet 350 Series Wireless Bridge is UL 2043 certified, and designed to achieve plenum rating as defined by various municipal fire codes.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 350 Series Ethernet Bridge	• Any company who needs to connect sites into a single LAN, even when separated by obstacles such as freeways, railroads and bodies of water that are normally inaccessible via cabling. • Business owners who want a low-cost, easy-to-deploy solution for connecting line-of-sight networks located in different buildings. • Business owners or IT directors who want multiple buildings on a campus to share a single high-speed line to the Internet.

Key Features

- High-speed (11-Mbps), high-power (100-mW) radios, delivering building-to-building links of up to 25 miles (40.2 km)
- A metal case for durability and plenum rating and an extended operating temperature rating for harsh environments
- Supports both point-to-point and point-to-multipoint configurations
- Broad range of supported antennas
- Simplified installation, improved performance, and upgradeable firmware, ensuring investment protection

Specifications

Feature	Cisco Aironet 350 Series Wireless Bridge
Data Rates Supported	1, 2, 5.5, and 11 Mbps
Frequency Band	2.4 to 2.497 GHz
Wireless Medium	Direct Sequence Spread Spectum (DSSS)
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	DBPSK @1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 and 11 Mbps
Operating Channels	North America: 11; ETSI: 13; Japan: 14
Nonoverlapping Channels	Three
Receive Sensitivity	1 Mbps: -94 dBm; 2 Mbps: -91 dBm; 5.5 Mbps: -89 dBm; 11 Mbps: -85 dBm
Delay Spread	1 Mbps: 500 ns; 2 Mbps: 400 ns; 5.5 Mbps: 300 ns; 11 Mbps: 140 ns
Available Transmit Power Settings[1]	100 mW (20 dBm); 50 mW (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm)
Range (typical, contingent upon antenna selected)	18 miles (28.9 km) @ 11 Mbps Up to 25 miles (40.2 km) @ 2 Mbps
Compliance	Operates license-free under FCC Part 15 and complies as a Class B device; complies with DOC regulations; complies with ETS 300.328, FTZ 2100, and MPT 1349 standards; complies with UL 2043 (The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local industry Canada office.)
SNMP Compliance	MIB I and MIB II
Antenna	Two RP-TNC connectors (antennas optional, none supplied with unit)
Encryption Key Length	128-bit
Security	128-bit WEP in bridge mode IEEE 802.11x (includes EAP and RADIUS) in AP mode
Status Indicators	Three indicators on the top panel provide information concerning association status, operation, error/warning, firmware upgrade, and configuration, network/modem, and radio status
Automatic Configuration Support	BOOTP and DHCP
Remote Configuration Support	Telnet, HTTP, FTP, TFTP, and SNMP
Local Configuration	Direct console port (with supplied serial cable)
Bridging Protocol	Spanning Tree
Dimensions	6.74 x 6.25 x 1.31 in. (17.1 x 15.9 x 3.3 cm)
Weight	1.43 lbs (.648 kg)
Environmental	Temperature: -4× to 131× F (-20× to 55× C) 10 to 90% (noncondensing)
Enclosure	Metal case (for plenumrating); UL 2043 certified
Input Power Requirements	24VDC 10% to 60 VDC (Ethernet line power)

[1] Maximum power setting will vary according to individual country regulations

Selected Part Numbers and Ordering Information[1]

Cisco Aironet 350 Series Wireless Bridge

AIR-BR350-x-K9	350 Series 11Mbps DSSS Bridge with 128-bit WEP

Cisco Aironet 350 Series Wireless Bridge Basic Maintenance

CON-SNT-PKG2	SMARTnet Maintenance for AIRBR350-A-K9

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet Antennas and Accessories

Every wireless Local Area Network (LAN) deployment is different. When engineering an in-building solution, varying facility sizes, construction materials, and interior divisions raise a host of transmission and multipath considerations. When implementing a building-to-building solution, distance, physical obstructions between facilities, and number of transmission points involved must be considered.

Cisco is committed to providing not only the best access points, client adapters, and bridges in the industry—it is also committed to providing a complete solution for any wireless LAN deployment. That is why Cisco has the widest range of antennas, cable, and accessories available from any wireless manufacturer.

With the Cisco FCC-approved directional and omnidirectional antennas, low-loss cable, mounting hardware, and other accessories, installers can customize a wireless solution that meets the requirements of even the most challenging applications.

Key Features

- Client Adapter Antennas—Cisco Aironet wireless client adapters come complete with standard antennas that provide sufficient range for most applications at 11 Mbps. To extend the transmission range for more specialized applications, a variety of optional, higher-gain antennas are provided that are compatible with selected client adapters
- Access Point Antennas—Cisco Aironet access point antennas are compatible with all Cisco RP-TNC-equipped access points. The antennas are available with different gain and range capabilities, beam widths, and form factors. Coupling the right antenna with the right access point allows for efficient coverage in any facility, as well as better reliability at higher data rates
- Bridge Antennas—Cisco Aironet bridge antennas allow for extraordinary transmission distances between two or more buildings. Available in directional configurations for point-to-point transmission and omnidirectional configuration for point-to-multipoint implementations, Cisco has a bridge antenna for every application
- Low-loss cable extends the length between any Cisco Aironet bridge and the antenna. With a loss of 6.7 dB per 100 feet (30m), low-loss cable provides installation flexibility without a significant sacrifice in range

Specifications

Client Adapter Antennas

Feature	AIR-ANT3351
Description	POS diversity dipole[1]
Application	Indoor diversity antenna[2] to extend the range of Aironet LMC client adapters
Approximate Indoor Range at 1 Mbps[3]	350 ft (107m)
Approximate Indoor Range at 11 Mbps[3]	100 ft. (51 m)
Cable Length	5 ft. (1.5m)
Dimensions	Base: 7 x 2 in. (18 x 5 cm) Height: 8 in. (20 cm)
Weight	9.2 oz. (261g)

1. A type of low-gain (2.2 dBi) antenna consisting of two (often internal) elements.
2. A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain and, as such, the more acute the angle of coverage.
3. All range estimations are based on an integrated client adapter antenna associating with an access point under ideal indoor conditions. The distances referenced here are approximations and should be used for estimation only.

Access Point Antennas

Feature	AIR-ANT5959	AIR-ANT3195	AIR-ANT2012	AIR-ANT3213
Description	Diversity omni-directional ceiling mount	3 dBi Patch Wall Mount Antenna	Diversity patch wall mount	Pillar mount diversity omni
Application	Indoor unobtrusive antenna, best for ceiling mount. Excellent throughput and coverage solution in high multipath cells and dense.	Indoor/Outdoor directional antenna	Indoor/Outdoor, unobtrusive medium range antenna	Indoor, unobtrusive medium-range antenna
Approximate Indoor Range at 1 Mbps[1]	350 ft. (105m)	Access Point: 271 ft. (82m) Bridge: .5 miles (.9 km)	547 ft. (167m)	497 ft. (151m)
Approximate Indoor Range at 11 Mbps[1]	130 ft. (45m)	Access Point: 80 ft. (24m) Bridge: 950 ft. (290m)	167 ft. (51m)	142 ft. (44m)
Cable Length	3 ft. (0.91m)	12 ft.	3 ft. (0.91m)	3 ft. (0.91m)
Dimensions	5.3 x 2.8 x 09. in. (13.5 x 7.1 x 2.3 cm)	4 x 5 in. (9.7 x 13 cm)	4.78 x 6.66 x .82 in. (12.14 x 16.92 x 2.08 cm)	10 x 1 in. (25.4 x 2.5 cm)
Weight	0.3 lbs. (0.14kg)	4.9 oz. (139g)	9.6 oz. (272g)	1 lb. (460g)

1. All range estimations are based on an integrated client adapter antenna associating with an access point under ideal indoor conditions. The distances referenced here are approximations and should be used for estimation only.

Access Point Antennas (cont.)

Feature	AIR-ANT1728	AIR-ANT4941	AIR-ANT3549	AIR-ANT1729
Description	High gain omnidirectional ceiling mount	2.2 dBi dipole antenna	Patch wall mount	Patch wall mount
Application	Indoor medium-range antenna, typically hung from crossbars of drop ceilings	Indoor omni-directional coverage	Indoor, unobtrusive, long-range antenna (may also be used as a medium-range bridge antenna)	Indoor, unobtrusive, medium-range antenna (may also be used as a medium-range bridge antenna)
Approximate Indoor Range at 1 Mbps[1]	497 ft. (151m)	350 ft.	Access Point: 700 ft. (213m) Bridge: 2.0 miles (3.2 km)	Access Point: 542 ft. (165m) Bridge: 1.1 miles (1.8 km)
Approximate Indoor Range at 11 Mbps[1]	142 ft. (44m)	130 ft.	Access Point: 200 ft. (61m) Bridge: 3390 ft. (1032m)	Access Point: 155 ft. (47m) Bridge: 1900 ft. (580m)
Cable Length	3 ft. (0.91m)	N/A	3 ft. (0.91m)	3 ft. (0.91m)
Dimensions	Length: 9 in. (22.86 cm) Diameter: 1 in. (2.5 cm)	5.5 in.	5 x 5 in. (12.4 x 12.4 cm)	4 x 5 in. (9.7 x 13 cm)
Weight	4.6 oz. (131g)	1.1 oz.	5.3 oz. (150g)	4.9 oz. (139g)

1. All range estimations are based on an integrated client adapter antenna associating with an access point under ideal indoor conditions. The distances referenced here are approximations and should be used for estimation only.

Bridge Antennas

Feature	AIR-ANT2506	AIR-ANT4121	AIR-ANT1949	AIR-ANT3338
Description	Omnidirectional Mast mount	High-gain omnidirectional Mast mount	Yagi mast mount	Solid dish
Application	Outdoor short-range point-to-multipoint applications	Outdoor medium-range point-to-multipoint applications	Outdoor medium-range directional connections	Outdoor long-range directional connections
Approximate Indoor Range at 1 Mbps[1]	5000 ft. (1525m)	4.6 miles (7.4 km)	6.5 miles (10.5 km)	25 miles (40 km)
Approximate Indoor Range at 11 Mbps[1]	1580 ft. (480m)	1.4 miles (2.3 km)	2.0 miles (3.3 km)	11.5 miles (18.5 km)
Cable Length	3 ft. (0.91m)	1 ft. (0.30m)	1.5 ft. (0.46m)	2 ft. (0.61m)
Dimensions	Length: 13 in. (33 cm) Diameter: 1 in. (2.5 cm)	Length: 40 in. (101 cm) Diameter: 1.3 in. (3 cm)	Length: 18 in. (46 cm) Diameter: 3 in. (7.6 cm)	Diameter 24 in. (61 cm)
Weight	6 oz. (17g)	1.5 lb. (0.68 kg)	1.5 lb. (0.68 kg)	11 lb. (5 kg)

[1] All range estimations are based on an integrated client adapter antenna associating with an access point under ideal indoor conditions. The distances referenced here are approximations and should be used for estimation only.

Low-Loss/Ultra Low-Loss Antenna Cable

Feature	AIR-CAB020LL-R	AIR-CAB050LL-R	AIR-CAB100ULL-R	AIR-CAB150ULL-R
Cable Length	20 ft. (6m)	50 ft. (15m)	100 ft. (30m)	150 ft. (46m)
Transmission Loss	1.3 dB	3.4 dB	4.4 dB	6.6 dB

Cisco Aironet Accessories

Feature	AIR-ACC2537-060	AIR-ACC3354	AIR-ACC2662
Description	60 in. (152 cm) bulkhead extender	Lightning arrestor	Yagi articulating mount
Application	Flexible antenna cable that extends access point cabling typically within an enclosure	Helps prevent damage due to lightning-induced surges or static electricity	Adds swiveling capability to mast-mounted yagi antennas

Selected Part Numbers and Ordering Information[1]

Cisco Aironet Accessories	
AIR-ACC2662	Yagi Antenna Articulating Mount
AIR-ACC3354	Lightning Arrestor w/ grounding ring
AIR-CAB020LL-R	20 ft. (6m) low-loss antenna cable
AIR-CAB050LL-R	50 ft. (15m) low loss antenna cable
AIR-CAB100ULL-R	100 ft. (30m) low loss antenna cable
AIR-CAB150ULL-R	150 ft. (46m) low loss antenna cable
Cisco Aironet Antennas	
AIR-ANT1728	5.2 dBi Omni Ceiling Mount Antenna
AIR-ANT1729	6 dBi Patch Wall Mount Antenna
AIR-ANT1949	13.5 dBi Yagi Mast Mount Antenna
AIR-ANT2012	6.5 dBi Diversity Patch Wall Mount Antenna
AIR-ANT2506	5.2 dBi Omnidirectional Mast Mount Antenna
AIR-ANT3195	3 dBi Patch Wall Mount Antenna
AIR-ANT3213	5.2 dBi Pillar-Mount Diversity Omni Antenna
AIR-ANT3338	21 dBi Solid Dish Antenna
AIR-ANT3351	2.2 dBi POS Diversity Dipole Antenna
AIR-ANT3549	8.5 dBi Hemispherical Patch Antenna
AIR-ANT4121	12 dBi Omnidirectional Mast Mount Antenna
AIR-ANT4941	2.2 dBi Dipole Antenna (Standard Rubber Duck)
AIR-ANT5959	2.0dBi Diversity Omni Ceiling Mount Antenna

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Aironet Antennas & Accessories Web site **http://www.cisco.com/go/antenna**

CHAPTER 4

IP Telephony, Video, & Web Collaboration

Campus IP Telephony, Video, & Web Collaboration at a Glance

Product	Features	Page
Cisco IP Phones IP 7900 Series	An exciting, distinctively stylish, and pure Voice over IP phone portfolio to meet the wide range of business communication needs at affordableprices • Display-based technologyprovides ease-of-use • Integratedinline power and 2-port Ethernet Switch provides end-to-end infrastructure integration • Rich application environment enabled byopen APIs based onXML	4-3
Cisco CallManager 3.3	• The software-based call processing and call controlcomponent of Cisco's IP Telephony solution • Resides on Cisco Media Convergence Servers (MCS), Cisco ICS7750, or selected third-party servers (CallManager 3.3)	4-4
CiscoWorks IP Telephony Environment Monitor	A suite of management applicationsthat helps ensure the readiness and manageability of convergednetworks that are supporting VoIP and IP telephonytraffic and applications. The bundle includes: • Voice Health Monitor • Default Fault Manager • CiscoView • CCO Downloadable Modules – IP Phone Information Utility – IP Phone Help Desk Utility. – Fault History Manager	9-18
Cisco IP Contact Center (IPCC) Enterprise Edition	Cisco IP Contact Center (IPCC) Enterprise Edition delivers intelligent callrouting, network-to-desktop CTI, and multi-channelmedia contact management to contact center agents over an IP network. It includes several applications, including thefollowing: • CallManager • Cisco Intelligent Contact Manager (ICM) • Cisco IP IVR/-IP Queue Manager	4-8
Cisco IP IVR	Cisco IP IVR, a new world interactive voice response (IVR) solution, provides a feature-rich foundation for the creation of an IP-based IVR that is open and expandable. Cisco IP IVR has the following key features: • Provides a multimedia (voice/data/Web) IP-empowered application-generation environment • Can be deployed anywhere in the IP network • Offers Web-based activation andadministration	4-10
Cisco IP Contact Center Express Edition (Formerly IP ICD)	• Cisco IPCC Express is a software-based ACD, IVR, and CTI applicationfor mid-sized contact centers with Cisco IP Telephony networks based on Cisco AVVID. • Cisco IPCC Express is an open systems platform allowing ease of configuration. • It has a graphically driven workflow editor providing a common interface for creating interactions, or call flows, and creates business logic between IVR and ACD functions.	4-9
Cisco Unity—Unified Messaging and Voice Mail	Voicemail and unifiedmessaging system delivers all messages into single inbox for access via phone, email or Internet	4-11
Cisco Personal Assistant	Software applicationallows users to browse voicemail, dial by name, and conferencefrom any phone using voice commandsinstead of telephone keypad via speech recognition	4-13
IP Telephony Applications	• Cisco Survivable Remote Site (SRS) Telephony Software—IOS software that runs on local branch office router provides IP Telephony backup redundancy for IP phonesin that office when IP phones detect thatWAN is down or/and CallManageris unreachable • Cisco IP Phone Messenger—sends Instant Messages (IM) between Cisco IP Phones and Lotus Sametime or MS Messenger desktop IM clients • Cisco IP SoftPhone—Windows-based applicationfor PC, allows users to make and receive calls from PC without a dedicated phone • Cisco Conference Connection (CCC)—enables enterprises to bring geographically dispersed employees and customers together to facilitate meetings and collaboration. CCC provides a cost-effective and time-efficientmethod of doing business without the hassle of travel.	4-14

Product	Features	Page
Cisco MCS 7800 Series Media Convergence Servers	High availability server platform for Cisco IP telephony systems • Turnkey solution, includes CallManager or oher software • For large- and medium-sized enterprise IP telephonydeployments	4-17
Cisco ICS 7750 Integrated Communications System	• A branch office/midmarket business with standalone IP telephonyneeds from 35-500 users • An end-user customer or partner who wants a single "box" (or platform) IP telephony solution to ease deployment and/or to standardize on voice configurationsacross multiple sites • An existing multiservice data networkcustomer who wants to add IP telephony functionality to create a converged network solution	4-18
Cisco IAD 2400 Series Integrated Access Device[1]	Business class fixed-configuration Integrated Access Device (IAD) • Delivers packet or TDM voice and data over single WAN uplink • IOS Telephony Service(ITS) provides local IAD-based call processing to offer key switch functionality ideal for small offices (5-24 phones) • IP-based keyswitch functionality ideal for small offices (5-20 phones) who do not need Cisco CallManager capabilities • Supports standard phonesand IP phones on a single platform • 8 FXS/16 FXS/16FXS+8FXO analog voice ports and 1 T1 digital voice port models • WAN Interfaces: T1- PPP, FR, ATM and DSL-ADSL and G.SHDSL	4-18
Cisco Voice Gateways[2]	The Cisco VG248 dedicated voice gatewayprovides connectivity between IP networks and legacy telephony systems/PSTN • Support various types of interfaces, including T1 and E1 • Fully manageable by Cisco CallManager, a CLI interface via Telnet, or via SNMP	4-22
Cisco IP/VC 3500 Series Videoconferencing Products	• Videoconferencing over IP solution • Cost-effective, easy-to-manage • Translates between H.323 and H.320 systems • Management and Qualty of Service	4-22
Cisco IP/TV 3400 Series Video Servers	• High-quality video communicationsover enterprise networks • Support live and scheduled video, video on demand • Enable training, corporate communications, business TV, and distance leaning	4-23
Cisco Web Collaboration Option	• Web-based colaboration, • Share any Windows desktop application • Ideal for both sales- and service-oriented customerservice organizations	4-24
Cisco E-mail Manager	• Automates the process of tracking and responding toinbound email. • Automatically assigns email requests to the most appropiate agent • Graphical rules engine makes it easy to define custom rules for the processing of email	4-25
Cisco Emergency Responder	• Works with Cisco CallManagerto automaticallyprovide E9-1-1 features in North America, and is compatible with any emergencynumber including 112 in Europe, 999 in UK, and 000 in Australia. • Dynamically tracks the location of IP phones, routes emergency calls to the appropriate E9-1-1 network, and provides the current location information to E9-1-1 call center dispatchers. • Provides real-time alert notificationsto on-site or contracted security groups, to facilitate a timely response to emergencysituations.	4-25
Cisco ATA Series of Analog Telephone Adaptors	Tums any analog telephone into an IP telephone. Each of the two voice ports supports independent telephone numbers providing two separate lines. • Interoperable with multiple standardsincluding H.323, SIP, MGCP and SCCP • Enables analog devices, such as phones and fax machines, to support Voice over IP services by converting the analog signalinto an IP signal	4-27
Cisco CTE-1400 Series Content Transformation Engine	Transforms Web content for display and interaction on small screen mobile devices and IP Telephones • Supports a broad range of devices • Transforms existing content • GUI/Console Administrative Tool	6-13

1. IP Keyswitch capabilities also available with 2600/2600XM and 3600 series routers; see IP Keyswitch Web site: http://www.cisco.com/go/keyswitch
2. Cisco's full line of multiservice routers also provide analog and digital voice gateway functionality through use of network modules and voice interface cards. Please see the 1700, 2600XM, 3600, 7200, 5x00 series in Chapter 1—Routers, as well as Chapter 7—Access Products.

Cisco 7900 Series IP Phones

Cisco IP Phones provide unmatched levels of integrated business functionality and converged communications beyond today's conventional voice systems. The Cisco IP Phone7960G "manager set" addresses the communication needs of the professional, with a high or busy amount of phone traffic. The Cisco IP Phone 7940G "business set" addresses the communication needs of a transaction type worker, in a office cubicle environment, who conducts medium to high telephone traffic. The Cisco IP Phone 7912G, 7910G+SW, 7910G, and 7905G "basic sets" address the communication needs of a cubicle worker who conducts low to medium telephone traffic. The Cisco IP Phone 7902G "entry set" addresses voice communication needs of a lobby, lab, manufacturing floor, and other areas where only a minimal amount of features are required. Cisco IP Phone Expansion Module 7914 extends the Cisco IP Phone 7960G with additional buttons and LCD, increasing the total number of buttons to 20 with one module, or 34 with two modules. Cisco IP Conference Station 7935, a high-quality hands-free conference station, is designed for use on desktops and offices and in small to medium-sized conference rooms.

Key Features

- Dynamic soft keys make the telephone simpler to use by presenting calling options based on context
- Open APIs using XML to deliver applications to the display
- Automatic phone discovery, VLAN configuration, and registration
- Quality of Service (QoS) is provided via support of 802.1pq, in addition to configurable DIFFSERV and TOS
- Voice-activity detection, silence suppression, comfort-noise generation, and error concealment
- G.711a, G.711u, G.729ab audio-compression coder-decoders (codecs)
- Software upgrade support via Trivial File Transfer Protocol (TFTP) server
- Microsoft NetMeeting enabled—features such as application sharing and video conferencing are available simply by pressing a button on your Cisco IP telephone
- Integrated Ethernet Switch supporting Ethernet connectivity for a downstream PC
- Integrated Inline power support allows the phone to receive power over the LAN
- A hearing-aid-compatible handset

Specifications

Feature	Cisco IP Phone 7902G	Cisco IP Phone 7905G	Cisco IP Phone 7910G and 7910G+SW	Cisco IP Phone 7912G	Cisco IP Phone 7940G	Cisco IP Phone 7960G	Cisco 7914 Expansion Module	Cisco IP Conference Station 7935
Display	None	Pixel-Based	Character-Based	Pixel-based	Pixel-Based	Pixel-Based	Pixel-based	Character-Based
Dynamic Soft Keys	0	4	0	4	4	4	N/A	0
Inline Power	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
10/100Base-T Ethernet Switch	No	No	Yes, 7910G+SW No, 7910G	Yes	Yes	Yes	N/A	No
Lines	1	1	1	1	2	6	14	1

Feature	Cisco IP Phone 7902G	Cisco IP Phone 7905G	Cisco IP Phone 7910G and 7910G+SW	Cisco IP Phone 7912G	Cisco IP Phone 7940G	Cisco IP Phone 7960G	Cisco 7914 Expansion Module	Cisco IP Conference Station 7935
Speaker Phone	No	Monitor Only	Monitor Only	Monitor Only	Yes	Yes	N/A	Yes
Headset Jack	No	No	No	No	Yes	Yes	N/A	No
3rd Party XML Applications	No	No	No	No	Yes	Yes	N/A	No

Selected Part Numbers and Ordering Information[1]

Cisco 7900 Series IP Power and Phones

CP-7960G	Cisco IP Phone 7960G, Manager Set
CP-7940G	Cisco IP Phone 7940G, Business Set
CP-7912G	Cisco IP Phone 7912G, Basic Set w/ Switch
CP-7910G+SW	Cisco IP Phone 7910G+SW, Basic Set w/ Switch
CP-7910G	Cisco IP Phone 7910G, Basic Set
CP-7905G	Cisco IP Phone 7905G, Basic Set
CP-7902G	Cisco IP Phone 7902G, Entry Set
CP-7935	Cisco IP ConferenceStation
CP-7914=	Cisco 7914 IP Phone Expansion Module for the 7960 IP Phone
CP-SINGLFOOTSTAND=	Single module footstand
CP-DOUBLFOOTSTAND=	Double module footstand
CP-WALLMOUNTKIT=	Non-Locking Wall Mount Kit for7910/40/60G series IP phones
CP-LCKNGWALLMOUNT=	Locking Wallmount Kit for the 7910/40/60G series IP phones
CP-PWR-CUBE=	IP Phone power transfomer for 7900 series IP phones
WS-PWR-PANEL	Catalyst 48 port Inline Power Patch Panel

[1] This is only a small subset of all parts. Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco IP Telephones Web site: **http://www.cisco.com/go/iptel**

Cisco CallManager 3.3

Cisco CallManager call-processing software extends enterprise telephony features and capabilities to enterprise LANs and packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems interact with the IP telephony solution through CallManager's open telephony application programming interfaces (API). Cisco CallManager is installed on the Cisco Media Convergence Server (MCS) and selected third-party servers. It ships with a suite of integrated voice applications and utilities, including the Cisco Attendant Console—a software-only manual attendant console; a conferencing application; and administrative reporting tools. For more VoIP network management features, see the CiscoWorks Manager IP Telephony Environment Monitor, page 9-18.

Cisco CallManager version 3.3 provides a scalable, distributable, and highly available enterprise IP telephony call-processing solution. Multiple servers are clustered and managed as a single entity; yielding scalability of up to 30,000 users per cluster. By interlinking multiple clusters, system capacity can be increased to as many as one million users in a 100-site system. Clustering aggregates the power of multiple, distributed Cisco CallManagers, enhancing the scalability and accessibility of the servers to phones, gateways, and applications. Triple call-processing server redundancy improves overall system availability.

The benefit of this distributed architecture is improved system availability and scalability. Call admission control ensures that voice quality of service (QoS) is maintained across constricted WAN links, and automatically diverts calls to alternative Public Switched Telephone Network (PSTN) routes when WAN bandwidth is not available. A Web-browsable interface to the configuration database enables remote device and system configuration.

Key Features

- Cisco CallManager includes a suite of integrated voice applications that perform voice conferencing and manual attendant console functions, eliminating the need for special-purpose voice processing hardware
- Supplementary and enhanced services such as hold, transfer, forward, conference, multiple line appearances, automatic route selection, speed dial, last-number redial, and other features are extended to IP phones and gateways
- Capabilities enhancements are achieved though software upgradeability, avoiding expensive hardware costs traditional to legacy PBX systems
- Cisco CallManager Attendant Console—This Web-enabled application supports the traditional role of a manual attendant console and allows the attendant to quickly accept and dispatch calls to enterprise users. An integrated directory service provides traditional busy lamp field (BLF) and direct station select (DSS) functions for any line in the system. It monitors the state of every line in the system without requiring hardware-based line monitoring devices, thereby saving costs
- Software-only applications such as the Cisco Interactive Voice Response system, Cisco IP Contact Center, Cisco Automated Attendant, and Cisco SoftPhone are applications that interact with the CallManager through telephony APIs

Specifications

Feature	Cisco CallManager 3.3[1]
Platforms	Media Convergence Server (MCS) Integrated Communications Serer (ICS-7750) Selected third-paty servers
Pre-Installed Software	Cisco CallManager version 3.3 (call processing and call-control application) Cisco CallManager version 3.3 configuration database (contains system and device configuation information, includingdial plan) Cisco CallManager Administration software Cisco Conference Bridge Cisco Attendant Console Bulk Administration Tool (BAT) CDR Analysis and Reporting (CAR) tool Real Time Monitoring Tool RTMT
Sample Subset of System Capabilities	H.323 scalability improvements - 1,000 H.323 calls per CallManager server in cluster Virus checker certification Cisco Intrusion Detection System (IDS) Host-Based Sensor certification

Feature	Cisco CallManager 3.3[1]
Summary of Administrative Features	Application discovery and registration to SNMPmanager
	Automated Alternate Routng Groups
	Bulk Administration
	Call Back
	Call Detail Records (CDR)
	Call forward reason code delivery
	Centralized, replcated configuration database, distributed Web-based management viewers
	Configurable and default ringer WAV files per phone
	Configuration database API
	Database automated change notification
	Date/time display format configurable per phone
	Debug information to common syslog file
	Device addition through wizards
	Device downloadable feature upgades—Phones, hardware transcoder resource, hardware conference bridge resource, VoIP gateway resource
	Device groups and pools for large system management
	Device mapping tool-IP address to MAC address
	Distinctive ring per line
	Dynamic Host Configuration Protocol (DHCP) block IP assignment-phones and gateways
	Dialed number translation table (inbound/outbound translation)
	Dialed Number Identification Service (DNIS)
	Enhanced 911 service
	H.323-compliant interface toH.323 clients, gateways, and gatekeepers
	Individual line Call Waiting Alert Configuration
	JTAPI 1.2 computer telephony interface
	LDAP version 3 directory interface to selected vendor's LDAP directories
	• Active Directory
	• Netscape Directory Server
	Manager Assistant
	Mappable softkeys
	MGCP signaling and control to selected Cisco VoIP gateways
	Multilevel Administration Access (MLA)
	Native supplementary services support to Cisco H.323 gateways
	Network Specific Facilities Paperless phone DNIS-display driven button labels on phones
	Performance monitoring SNMP statistics from applications to SNMP manager or to operating system
	Performance Monitor
	QoS statistics recorded per call
	QSIG Support
	Redirected DNIS (RDNIS), inbound, outbound (to H.323 devices)
	Select specifiedline appearance to ring; Select specified phone to ring
	Single CDR per cluster
	Single point system/device configuration
	Sortable component inventory list by device, user, or line
	System event reporting-to common syslog or operating system event viewer
	TAPI 2.1 computer telephony interface
	Time-zone configurable per phone
	XML API into IP phones (794X/6X)
	Zero cost automated phone moves; Zero cost phoneadds

Feature	Cisco CallManager 3.3[1]
Summary of User Features	Answer/answer release
	Auto-answer/[2]intercom
	Call connection
	Call coverage
	Call forward-all (off-net/on-net); Call forward-busy; Call forward-no answer
	Call hold/retrieve
	Call park/pickup; Call pickup group-universal
	Call status per line (state, duration, number)
	Call waiting/retrieve
	Calling Line Identification (CLID); Calling party name identification (CNID)
	Calling Line Identifiation Restriction (CLIR)
	Direct inward dial (DID; Direct outward dial (DOD)
	Directory dial from phone-corporate, [2]personal
	Directories-missed, placed, received calls list stored on selected IP phones
	Distinctive ring (on-net vs. off-net); Distinctive ring per phone
	Drop last conference party(ad-hoc conferences)
	Extension mobility support
	Hands-free, full-duplex speakerphone
	HTML help access from phone
	Last number redial (off-net/on-net)
	Message waiting indication
	Multiparty conference-Ad-hoc with add-on, Meet-me
	Multiple line appearances per phone
	Music-on-hold
	Mute capability from speakerphone and handset
	On-hook dialing
	Operator attendant-Web-browser interface, loop key notification, logon/logoff, busy/available, left/right hand access, headphone access, busy lamp field, direct station select, drag and drop transfer, call status (state, duration, and number)
	Privacy
	Real-time QoS statistics through http browse to phone
	Recent dial list-calls to phone, calls from phone, auto-dial, and edit dial
	Single button data collaboration on SoftPhone-chat, whiteboard, and app sharing
	Single directory number, multiple phones-bridged line appearances
	Speed dial-multiple speed dials per phone
	Station volume controls (audio, ringer)
	Transfer-with consultation hold
	User-configured speed dial and call forward through Web access
	Web services access from phone
	Wideband audio codec support—proprietary 16-bit resolution, 16 kHz sampling rate codec

1. Additional RAM may be required in Media Convergence Servers to support existing and enhanced services in Cisco CallManager 3.3.
2. Indicates new feature or service for Cisco CallManager version 3.3

For More Information

See the Cisco CallManager Web sites: **http://www.cisco.com/go/callmgr**

Cisco IP Contact Center (IPCC) Enterprise Edition

Cisco IP Contact Center (IPCC) Enterprise Edition delivers intelligent contact routing, call treatment, network-to-desktop computer telephony integration (CTI), and multi-channel contact management over an IP infrastructure. By combining multi-channel automatic call distributor (ACD) functionality with IP telephony in a unified solution, Cisco IPCC Enterprise enables companies to rapidly deploy a distributed contact center infrastructure.

Cisco IPCC Enterprise Edition segments customers, monitors resource availability, and delivers each contact to the most appropriate resource anywhere in the enterprise. The software profiles each customer using contact-related data such as dialed number and calling line ID, caller-entered digits, data submitted on a Web form, and information obtained from a customer profile database lookup. At the same time, the system knows which resources are available to meet the customer's needs based on real-time conditions (agent skills and availability, interactive voice response [IVR] status, queue lengths, and so on) continuously gathered from various contact center components.

Cisco IPCC Enterprise provides a state of the art VoIP contact center solution that allows seamless integration of inbound and outbound voice applications with Internet applications including real-time chat, Web collaboration and e-mail. This integration allows for unified capabilities, enabling a single agent to support multiple interactions simultaneously regardless of the communications channel the customer has chosen. Since each interaction is unique and may require individualized service, Cisco provides contact center solutions to manage each interaction based on virtually any contact attribute.

Furthermore, Cisco can bridge the gap between TDM and IP infrastructures, providing a seamless integration of voice, chat, e-mail, and Web collaboration applications over both of these technology platforms. This allows companies to preserve the value of their existing investments in call center products such as ACDs, IVRs, PBXs, etc. while leveraging Cisco's wide range of solutions to support the same contact center requirements in a converged network environment.

Key Features[1]

- Full Scalability from less than a hundred to thousands of seats
- Multi-channel interaction—Web collaboration with chat and callback, email, voice mail and fax routing
- Multi-site Contact Centers support; CRM Integration
- Cradle-to-grave contact call detail records
- Common agent and supervisor desktops across all Cisco customer interaction management products
- Pre-defined and custom historical reports; Real-time reports integrated in the agent and supervisor desktops
- Support for custom call treatment for calls in queue includes support for music in queue and custom messaging
- Standard screen pop allows any caller-entered information to be popped to the agent
- Full support for agent/supervisor interaction via chat
- Ability to pre-define agent-supervisor messages

[1] Abbreviated list of IPCC Features

Selected Part Numbers and Ordering Information[1]

Cisco IP Contact Center	
IPC-Bundle	Includes - ICM, 1 Call Manager PG, 1 IVR PG, 24 Agent Desktop Licenses, 1 Supervisor Desktop License, 1 System Manager AWS – full, 1 full documentation set plus on-line documentation
IPC-AGTCTD-L	Cisco Toolkit Desktop For IPCC License
IPC-SUPCTS-L	Cisco Toolkit Supervisor For IPCC License
IPC-AGTCAD-L	Cisco Agent Desktop For IPCC License
IPC-AGTCADCTI-L	Cisco Agent Desktop For IPCC With CTI License
IPC-SUPCSD-L	Cisco Supervisor Desktop For IPCC License

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco IPCC Enterprise Edition Web site: **http://www.cisco.com/go/ipcc**

Cisco IPCC Express Edition (Formerly IP ICD)

Cisco IPCC Express Edition is an inexpensive, easy-to-install, and easy-to-use automatic call distributor (ACD) for enterprise organizations. It is seamlessly integrated with all other customer response applications, including Cisco IP Interactive Voice Response (IP IVR) and Cisco IP Automated Attendant (IP AA). Key benefits of IPCC Express include: it provides a low-cost, entry-level ACD that is easy to install, administer, and use; it supports multimedia (voice, data, and Web) access when used with Cisco IP IVR; it provides complete customization tools for call flow scripts; and it supports seamless integration with Cisco customer response applications.

Cisco IPCC Express is available as two packages: Cisco IPCC Express Standard and Cisco IPCC Express Enhanced. The Standard version is priced for entry-level users, allowing you to capture opportunities in the small and medium-size business market segment. The Enhanced version offers a full-featured ACD for entry- to mid-size contact centers. The Enhanced version also provides a migration pathway to Cisco IP Contact Center (IPCC), Cisco's premier contact center product.

Key Features[1]

- Browser-based Cisco IPCC Express administration is fully integrated with Cisco CallManager browser-based administration
- Cradle-to-grave contact call detail records
- Standard screen allows any caller-entered information to be popped to the agent
- Pre-defined or custom historical reports
- Real-time reports within the agent and supervisor desktops
- Common agent and supervisor desktops across all Cisco customer interaction management products including Cisco IPCC Express Standard, Enhanced and Cisco IP Contact Center Enterprise (formerly IPCC)
- Localization
- Full support for agent/supervisor interaction via chat; Ability to pre-define agent-supervisor messages
- Full IP call queue points and prompt; Collect voice interaction capabilities
- Optional Automatic Speech Recognition (ASR) and Text to Speech (TTS) capabilities
- Support for custom call treatment such as music for calls in queue

[1] **Abbreviated list of IPCC Features**

Selected Part Numbers and Ordering Information[1]

Cisco IP Integrated Contact Distribution (ICD)

ICD-3.0-STD-BS SW	Standard ICD 3.0 Standard Bundle
ICD-3.0-STD-BB	Bid Set ICD 3.0 Standard Bundle
ICD-3.X-S-AGT1	1 Cisco Standard Agent Desktop ICD 3.X
ICD-3.X-S-AGT5	5 Cisco Standard Agent Desktops ICD 3.X
ICD-3.X-S-AGT10	10 Cisco Standard Agent Desktops ICD 3.X
ICD-3.X-S-AGT25	25 Cisco Standard Agent Desktops ICD 3.X
ICD-3.X-S-AGT50	50 Cisco Standard Agent Desktops ICD 3.X
ICD-3.X-S-SUP1	1 Cisco Standard Supervisor Desktop ICD 3.X
ICD-3.X-S-HIST1	1 Cisco Standard Historical Reporting ICD 3.X
ICD-3.0-ENH-BS	ICD 3.0 Enhanced Bundle
ICD-3.X-E-AGT1	1 Cisco Enhanced Agent Desktop ICD 3.X
ICD-3.X-E-AGT5	5 Cisco Enhanced Agent Desktops ICD 3.X
ICD-3.X-E-AGT10	10 Cisco Enhanced Agent Desktops ICD 3.X
ICD-3.X-E-AGT25	25 Cisco Enhanced Agent Desktops ICD 3.X
ICD-3.X-E-AGT50	50 Cisco Enhanced Agent Desktops ICD 3.X
ICD-3.X-E-SUP1	1 Cisco Enhanced Supervisor Desktop ICD 3.X
ICD-3.X-E-HIST1	1 Cisco Enhanced Historical Reporting ICD 3.X

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco IP Integrated Contact Distribution Web site:
http://www.cisco.com/go/icd

Cisco IP IVR

Cisco IP IVR, an interactive voice response (IVR) solution, provides a feature rich foundation for the creation of an IP-based Cisco IP IVR that is open and expandable. Written in Java to provide customer flexibility, IVR includes the following features:

- Multimedia (voice/data/Web) IP-empowered application-generation environment
- Support for optional Automated Speech Recognition (ASR) and Text-to-Speech (TTS)
- Support for VoiceXML
- Multiple Language support
- Cisco IP IVR can be located in anywhere the IP network
- Offers web-based activation and administration
- Flows (the IP IVR applications) are stored in an industry standard LDAP directory
- Cisco IP IVR is sold with Cisco CallManager and can be co-resident on the same server as CallManager or can function on a separate, dedicated media convergence servers (MCSs) or Cisco-approved customer provided server
- Packages available to scale up to 60 ports
- Cisco IP IVR offers enhanced scalability

Cisco Unity—Unified Messaging and Voice Mail

Cisco Unity is a powerful Unified Communications server that provides advanced, convergence-based communication services and integrates them with the desktop applications business professionals use everyday, improving customer service and productivity. Designed for enterprise-scale organizations, Cisco Unity delivers unified messaging that gives subscribers the ability to access and manage messages and calls from anywhere, at any time, regardless of device or media type. Subscribers can listen to e-mail over the telephone, check voice messages from the Internet, and if a fax server is present, forward faxes to any local fax machine. Cisco Unity voice messaging features robust automated attendant functionality that includes intelligent routing, and easily customizable call screening and message notification options. Cisco Unity supports localized versions in multiple languages and supports multiple languages on a single system.

Cisco Unity's optional digital networking module enables connectivity to other Cisco Unity servers at the same site via the LAN or remotely via WAN. Digital networking gives users the ability to send subscriber-to-subscriber messages anywhere in the world.

Cisco Unity supports both Cisco CallManager and leading legacy telephone systems—even simultaneously—to help smooth the transition to IP telephony and protect existing infrastructure investments. Built on a scalable platform, it uses streaming media and an intuitive HTML browser-style system administration interface. Costs are minimized when Cisco Unity's server architecture is truly unified with an organization's data network.

Key Features

- Architecture allows IT staff to set one back-up procedure, one message storage policy, and one security policy
- Enhanced scalability allows up to 72 ports per server; up to 7,500 subscribers per server; or a total of 250,000 users in an Exchange environment or 100,000 users in a Domino environment
- Support for Exchange 2000/Active Directory as the single message store and directory; AMIS-A and VPIM interoperability for Exchange systems
- Enhanced networking for large deployments—support for complex TDM telephone networks (multiple dialing domains)
- Support for multiple CCM clusters; ability to light Message Waiting Indicators
- With Exchange/Domino off-line, utilizes pre-MTA queue to take messages and give basic message access; Support for Lotus Domino as the single message store
- Fault-tolerant system tools—robust security, file replication, event logging, and optional software RAID levels 0-5
- Support for Windows 2000[1] in a mixed/native mode
- Unity Inbox/VMI (Visual Messaging Interface) is an Internet Explorer-based voice mail inbox providing unified messaging
- Unity Bridge provides advanced message interchange functionality with legacy Avaya/Octel voice mail systems—unlocking proprietary networking to deliver open standards-based IP migration

[1] Unity will not support Windows NT on the Unity server, although it can be installed into an NT environment.

Specifications

Feature	Cisco Unity 3.1
Unity Voice Mail (VM) and Unified Messaging (UM) Possible Configurations	16, 32 and Max sessions Configured for CallManageror configuredfor legacy PBX/dual integration[1]
Options	Voice Mail; Voice Mail with Multi-lingual option; Unified Messaging with Text-to-Speech (TTS) option Unified Messaging with Multi-lingual option; Exchange or Domino; AMIS for Exchange; VPIM for Exchange; Unity Inbox/Visual Messaging Interface; Failover for Exchange; Unity-Bridge for Exchange

[1] Contact your Cisco Software Sales Representative for Integration information.

Selected Part Numbers and Ordering Information[1]

Cisco Unity Servers	
UNITY-SVR1400-1A	Dell 1400; rack-mountable; (W2K included)
UNITY-SVR2500A-1A	Dell 2500; rack-mount; 512MB; RAID 1 (W2K included)
UNITY-SVR2500C-2A	Dell 2500; rack-mount; 1GB; RAID 5, 2nd CPU, Win2K
UNITY-SVRX232-1A	IBM x232 rack; 512MB; RAID 1 (W2K included)
UNITY-SVRX232-2A	IBM x232 rack; 1GB; RAID 5, 2nd CPU (W2K included)
UNITY-SVRL570-1A	Compaq ML570 rack; 2GB; RAID 1(x2), RAID 5, Dual CPU, Win2K
UNITY-SVRL570-2A	Compaq ML570 rack; 4GB; RAID 1(x2), RAID 5, Quad CPU, Win2K
UNITY-SVR7827-1A	MCS 7827 rack:(W2K included)
UNITY-SVR7837-1A	MCS 7837 rack; 512MB; RAID 1 (W2K included)
UNITY-SVR7847-2A	MCS 7847 rack; 1GB; RAID 5, 2nd CPU (W2K included)
UNITY-EXP-CHAS=	Expansion chassis
Cisco Unity 3.1 Unified Messaging and Voicemail Software	
UNITYU50-4-3.1=	Unity Unified Messaging, 50 users (includes 4 sessions)
UNITYU100-8-3.1=	Unity Unified Messaging, 100 users (includes 8 sessions)
UNITYU200-12-3.1=	Unity Unified Messaging, 200 users (includes 12 sessions)
UNITYU300-16-3.1=	Unity Unified Messaging, 300 users (includes 16 sessions)
UNITYU500-24-3.1=	Unity Unified Messaging, 500 users (includes 24 sessions)
UNITYU875-32-3.1=	Unity Unified Messaging, 875 users (includes 32 sessions)
UNITYU1175-40-3.1=	Unity Unified Messaging, 1175 users (includes 40 sessions)
UNITYU1600-48-3.1=	Unity Unified Messaging, 1600 users (includes 48 sessions)
UNITYU2200-60-3.1=	Unity Unified Messaging, 2200 users (includes 60 sessions)
UNITYU2950-72-3.1=	Unity Unified Messaging, 2950 users (includes 72 sessions)
UNITYV50-4-3.1=	Unity Voice Messaging, 50 users (includes 4 sessions)
UNITYV100-8-3.1=	Unity Voice Messaging, 100 users (includes 8 sessions)
UNITYV200-12-3.1=	Unity Voice Messaging, 200 users (includes 12 sessions)
UNITYV300-16-3.1=	Unity Voice Messaging, 300 users (includes 16 sessions)
UNITYV500-24-3.1=	Unity Voice Messaging, 500 users (includes 24 sessions)
UNITYV875-32-3.1=	Unity Voice Messaging, 875 users (includes 32 sessions)
UNITYV1175-40-3.1=	Unity Voice Messaging, 1175 users (includes 40 sessions)
UNITYV1600-48-3.1=	Unity Voice Messaging, 1600 users (includes 48 sessions)
UNITYV2200-60-3.1=	Unity Voice Messaging, 2200 users (includes 60 sessions)
UNITYV2950-72-3.1=	Unity Voice Messaging, 2950 users (includes 72 sessions)
Cisco Unity Languages and Real Speak TTS	
UNITY-RS-2ML=	Unity, 2-port Real Speak TTS, US Eng, UK, F, Ger, Euro Sp
UNITY-RS-4ML=	Unity, 4-port Real Speak TTS. US Eng, UK, F, Ger, Euro Sp
UNITY-RS-6ML=	Unity, 6-port Real Speak TTS. US Eng, UK, F, Ger, Euro Sp
UNITY-MULTILANG=	Multiple Language support
UNITY-TWOLANG=	Add support for a second language
UNITY-AMIS=	Unity, AMIS-A networking

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco Unity site: **http://www.cisco.com/go/unity**

Cisco Personal Assistant

Cisco Personal Assistant streamlines communications with personal call rules, speech recognition, and productivity services for IP phones. As an integral part of Cisco AVVID (Architecture for Voice, Video and Integrated Data), it interoperates with Cisco CallManager and scales to meet the present and future needs of your employees. Users can access voice mail, dial by name, and conference from any telephone using speech recognition instead of the telephone keypad. The Web-based and telephone user administration interfaces allow users to forward and screen calls in advance or in real time. The phone services enable users to check e-mail, voice mail, calendar, and personal contact information using the large, pixel-based LCD and interactive soft keys on the Cisco IP Phone 7940 or 7960.

Key Features

- Ubiquitous Access: Cisco Personal Assistant with Speech Recognition and IP Phone Productivity Services integrate with Cisco CallManager, Cisco Unity, and Microsoft Exchange within Cisco AVVID to streamline communications
- Automatic Speech Recognition (ASR): Speech recognition interface allows users to utilize simple voice commands to perform tasks such as retrieval, replying, recording, and deletion of voice messages; Entries can be dialed from personal address books or the corporate enterprise Lightweight Directory Access Protocol (LDAP) directory; Users can synchronize their Microsoft Exchange contact lists with their personal address books for quick name-dialing and ad-hoc group conferencing; Access to sensitive features such as voice mail is controlled by user authentication
- Manage Inbound and Outbound Calls (Rules-Based Routing): Using a Web interface to create rules, users can forward and screen calls based on caller identification, time of day, and meeting schedules; With "follow me," a special rule that uses speech recognition, users can forward all calls to a phone number immediately; Users can activate sets of pre-created rules from any telephone
- CalendarView: Users can keep track of appointments right on the IP phone, directly from the Microsoft Exchange server with no synchronization necessary. In addition, users can choose to be notified of an upcoming event on the phone display or by pager
- MailView: Cisco Personal Assistant presents users with access to e-mail and Cisco Unity voice-mail messages in the inboxes on the corporate messaging server. Users can access messages from a conference room, lobby phone, or colleague's phone, as well as their own. Any operation performed on the messages using MailView is automatically reflected in Microsoft Exchange and Cisco Unity; Cisco Personal Assistant interfaces with Microsoft Exchange and IMAP 4 message stores for MailView features.

Specifications

Feature	Cisco Personal Assistant
Platform	Cisco Media Convergence Server MCS-7825H-2.2-EVV1 and MCS-7835H-2.4-EVV1
Web Server Requirements for IP Phone Productivity Services Platform	Basic Web Server: Microsoft IIS 4.0 or later Separate server for Cisco Personal Assistant Server and Speech Recognition Server
Software Compatibility	Cisco CallManager 3.1+. 3.2+, and 3.3+ Cisco Unity 2.46+,3.0+, and 4.0+ for voice-mail features Microsoft Exchange 5.5 and Exchange 2000 for calendar, e-mail, contact synchronization features

Selected Part Numbers and Ordering Information[1]

Cisco Personal Assistant	
SW-PASR1.3-SVR2S	Cisco Personal Assistant 1.2 Server Software with Speech Recognition[2]
SW-PERSPROD-USR=	Personal ProductivityUser License
SW-PERSPROD-USR10=	Personal Productivity 10 User License
SW-PASR1-KX=	Cisco Personal Assistant 1.2, Expansion Speech Recognition Session[3]

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

[2] Cisco Personal Assistant can be purchased with an MCS-7825H-2.2-EVV1 or an MCS-7835H-2.4-EVV1 media convergence server.

[3] Various session combinations available.

For More Information

See the Cisco Personal Assistant Web site: **http://www.cisco.com/go/personalassist**

Additional Cisco IP Telephony Applications

Cisco SRS Telephony

Survivable Remote Site Telephony (SRS Telephony) provides key backup telephony functions at remote branch office routers if connectivity to the centrally-located Cisco CallManager fails (i.e. WAN link is interrupted). In this case the SRS Telephony-enabled router will take over and provide basic telephony service (including off-net calls to 911). Introduced in Cisco IOS Release 12.1.5YD, the application is ideal for enterprise organizations looking to cost-effectively deploy IP telephony in their branch office location. Cisco IOS Release 12.2(13)T added SRS Telephony 2.0 features on Cisco 1751, 1760, 2600, 2600 XM, 2691, 3600, 3725/3745, IAD 2400, Catalyst 4000 AGM, and Cisco 7200 series of routers. SRS Telephony 2.1 features are available in 12.2(11)YT on Cisco 1751, 1760, 2650, 2600XM, 2691, 3640/3640A, 3660, and Cisco 3725/3745 routers.

SRS Telephony 2.0 features: Huntstop support; Music/Tone on Hold; Class of Restriction; Distinctive Ringing; Global forwarding to voicemail across PSTN during Cisco CallManager fallback; TCL based simple AA and IVR on local gateway (SRS Telephony router); Transfer across H323 network of Cisco endpoints; Alias lists for single number to be designated for unregistered phones

SRS Telephony 2.1 features: International language support; Call forward no-answer/busy to Unity server with Personal Greeting; Cisco 7914 and 7935 support; VG248 support

For More Information

See the Cisco SRS Telephony Web site: **http://www.cisco.com/go/srs**

Cisco IP Phone Messenger

The Cisco IP Phone Messenger (IPPM) is a productivity application, providing enhanced, real-time collaboration for Cisco AVVID IP Communications systems. Cisco IPPM extends the benefits of Instant Messaging and Presence to Cisco CallManager networks, allowing users to send and receive instant messages on Cisco 7940 and 7960 IP phones. Cisco IPPM interworks with IBM Lotus Sametime and MSN Messenger clients and supports the IETF SIMPLE (RFC-3428) protocol for instant messaging and presence. IPPM 1.1 requires Cisco CallManager release 3.2 or later and is supported on the Cisco 7825 and 7835 Series Media Convergence Servers.

For More Information

See the Cisco IP Communications Web site:
http://www.cisco.com/go/ipcommunications

Cisco IP SoftPhone

Cisco IP SoftPhone 1.3 is a PC based application that allows you to use your phone extension from wherever you connect to your corporate IP network, even over the Internet when using a VPN client.

It's dual mode operation allows you to either control a physical IP phone, or perform all the functions of a phone in standalone mode using your PC's soundcard or a USB audio handset or headset.

Selected Part Numbers and Ordering Information[1]

Cisco Survivable Remote Site Telephony (SRS Telephony) Licenses	
FL-SRST-SMALL	SRS Telephony Site License for the Cisco IAD 2400/2600/3620/Catalyst 4224 (up to 24 phones)
FL-SRST-MEDIUM	SRS Telephony Site License for the Cisco 3640 (up to 48 phones) or order multiple licenses for the Cisco 3660 (up to 144 phones, each supports up to 48 phones)
Cisco IP SoftPhone	
SW-IPSOFTPHONE25=	Cisco IP Softphone CD; 25 licenses (licenses also available for 1, 50, and 100 users)

For More Information

See the Cisco IP SoftPhone Web site: **http://www.cisco.com/go/softphone**

Cisco IP Manager Assistant[1]

Cisco IP Manager Assistant is a tool that allows an assistant to provide call coverage for up to five managers simultaneously. When a user is configured as an IPMA manager, they are associated with a primary and secondary assistant. The configured manager is always logged onto the service and selects the preferred assistant from the 7960 services menu. Features available to the manager are initiated from softkeys on the manage's phone. Assistant user features are initiated and managed from a PC-based application named the Assistant Console.

[1] IP Manager Assistant is available as part of Cisco CallManager 3.3 for no additional charge.

Key Features

- Manager tools: 7960 IP phone—selection of assistant from pre-configured list; Divert All, Immediate Divert, Transfer to Voice Mail, Intercept, DND, SetWatch, Assistant Watch, Call Filtering feature invocation; display of toggled feature status for Divert All, Filtering, DND, Assistant Watch and Assistant availability; speed dial and line appearance configuration for intercom functionality; Manager Desktop—secure, browser-based access to configuration for default assistant assignment, Divert All target, Immediate Divert target and filter list (CLID) configuration.
- Admin Assistant Tools: 7960 IP Phone/7914 line extender—speed dial and line appearance configuration for intercom functionality; 7960 IP phone—invocation of new softkey features including Transfer to Voice Mail and Immediate Divert, speed dial to manager's intercom line; Assistant Console application—Windows application installed on assistant PC. GUI consistent with CallManager Attendant Console application. User-sizable application window and panes

Specifications

Feature	Cisco IP Manager Assistant
Platform	Media Convergence Server (MCS)
Software Compatibility	Cisco CallManager version 3.3 Assistant ConsoleApplication—Microsoft Windows98, NT desktop, ME, 2000 Desktop and XP

For More Information

See the Cisco Media Convergence Server Web site: **http://www.cisco.com/go/ipma**

Cisco Conference Connection

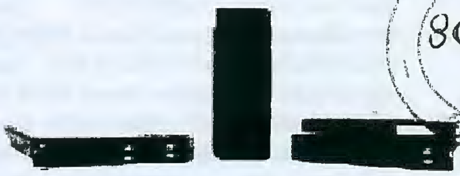
Cisco Conference Connection (CCC) is designed for small to medium enterprises and remote offices of larger enterprises. Cisco Conference Connection facilitates relevant participation regardless of location, enables faster decisions, and eliminates travel cost and time and disruptions caused by requirements for a physical conference room presence. Typical applications include service calls, project management, sales reviews, corporate announcements, customer and employee training, and other business meetings. This application is ideal for enterprieses trying to increase productivity while reducing expense. Simple web-based interface enables employees to manage their conference schedules and eliminates the service charges to conference service providers.

For More Information

See the Cisco Conference Connection Web site:
http://www.cisco.com/en/US/products/sw/voicesw/ps752/index.html

Cisco MCS 7800 Series Media Convergence Servers

Cisco MCS 7815I-2000



The Cisco MCS 7815I-2000 provides an entry level tower server equipped with an Intel Pentium™ 4 2000MHz processor, 40GB ATA hard drive and single non-hot swap power supply. An optional tape backup is available on some models of the MCS 7815I-2000.

Cisco MCS 7825H-2266

The Cisco MCS 7825H-2266 provides an entry level rack mount server that occupies only one rack mounting space. This server is equipped with an Intel Pentium™ 4 2266MHz processor, 40GB ATA hard drive and a single non-hot swap power supply. An optional tape backup is available on some models of the MCS 7825H-2266.

Cisco MCS 7835H-2400 and Cisco MCS 7835I-2400

These Cisco MCS platforms provide a highly available mid-level rack mounted server solution that is equipped with an Intel Prestonia Xeon™ 2400MHz processor, up to six hot-swap Small Computer Systems Interface (SCSI) hard disks, a Redundant Array of Independent Disks (RAID) 1/0 Controller, hot swap fans and redundant hot swap power supplies. An optional tape backup is available for some models of the MCS 7835H-2400 and MCS 7835I-2400.

Cisco MCS 7845H-2400 and Cisco MCS 7845I-2400

These Cisco MCS platforms provide a powerful and highly reliable high level rack mounted server solution that is equipped with two Intel Prestonia Xeon™ 2400MHz processors, up to six hot-swap SCSI hard disks, RAID 1/0 controller, redundant hot swap fans and redundant hot swap power supplies. An optional tape backup is available for some models of the MCS 7845H-2400 and MCS 7845I-2400.

Specifications

Cisco MCS-7815I-2000	Cisco MCS-7825H-1266	Cisco MCS-7835H-2400	Cisco MCS-7835I-2400	Cisco MCS 7845H-2400	Cisco MCS 7845I-2400
Intel Pentium® 4 2000-MHz processor 512KB L2 Cache 512MB SDRAM 40GB ATA/100 Hard Disk 1.44MB Floppy Disk DVD Drive Integrated ATA Controller Single 10/100/1000 Ethernet NIC Tower System with optional rack mount kit.	Intel Pentium® 2266-MHz processor 512KB L2 CacheSDRAM is configuration dependant Hard Disk is configuration dependant 1.44MB Floppy Disk DVD Drive Hard Disk Controller is configuration dependant Dual 10/100/1000 Ethernet NIC1U Rack Mount System	Intel Xeon® 2400-MHz processor 512KB Cache SDRAM is configuration dependant Hard Disk is configuration dependant SCSI Controller. Dual 10/100/1000 Ethernet NIC2U Rack Mount System.	IntelXeon® 2400-MHz processor 512KB Cache SDRAM is configuration dependant Hard Disk is configuration dependant SCSI Controller. Dual 10/100/1000 Ethernet NIC2U Rack Mount System	Dual Intel Xeon® 2400-MHz processor 512KB Cache SDRAM is configuration dependant Hard Disk is configuration dependant SCSI Controller. Dual 10/100/1000 EthernetNIC2U Rack Mount System	Dual Intel Xeon® 2400-MHz processor 512KB Cache SDRAM is configuration dependant Hard Disk is configuration dependant SCSI Controller. Dual 10/100/1000 EthernetNIC2U Rack Mount System

Selected Part Numbers and Ordering Information[1]

Cisco Media Convergence Server 7815I-20001[1]	
MCS-7815I-2.0-EVV1; CS-7815I-2.0-ECS1	Cisco Media ConvergenceServer 7815I-2000
Cisco Media Convergence Server 7825H-2266	
MCS-7825H-2.2-EVV1; MCS-7825H-2.2-ECS1	Cisco Media Convergence Server 7825H-2266
Cisco Media Convergence Server 7835H-2400	
MCS-7835H-2.4-EVV1; MCS-7835H-2.4-ECS1	Cisco Media Convergence Server 7835H-2400
Cisco Media Convergence Server 7835I-2400	
MCS-7835I-2.4-EVV1; MCS-7835I-2.4-ECS1	Cisco Media ConvergenceServer 7835I-2400
Cisco Media Convergence Server 7845H-2400	
MCS-7845H-2.4-EVV1; MCS-7845H-2.4-ECS1; MCS-7845H-2.4-ECS2	Cisco Media ConvergenceServer 7845H-2400
Cisco Media Convergence Server 7845I-2400	
MCS-7845I-2.4-ECS1; MCS-7845I-2.4-ECS2	Cisco Media ConvergenceServer 7845I-2400
Cisco Media Convergence Server 7855I-1500	
MCS-7855I-1.5-ECS1; MCS-7855I-1.5-ECS2	Cisco Media ConvergenceServer 7855I-1500
Cisco Media Convergence Server 7865I-1500	
MCS-7865I-1.5-ECS1; MCS-7855I-1.5-ECS2	Cisco Media ConvergenceServer 7865I-1500

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Media Convergence Server Web site: **http://www.cisco.com/go/mcs**

Cisco ICS 7750 Integrated Communications System

The Cisco Integrated Communications System (ICS) 7750 is a versatile IP telephony and services solution that brings the benefits of converged IP services to midmarket businesses and enterprise branch offices. Call processing, voice applications, voice gateways and multiservice IP routing are integrated within the system chassis to deliver true convergence while enhancing system manageability. The modular system architecture enables expansion of call processing redundancy, voice gateway capacity, routing capacity, and IP services to deliver system availability and scalability. The ICS 7750 offers quick and cost-effective deployment of powerful applications including unified messaging, integrated Web call centers, and data/voice collaboration.

The Cisco ICS 7750 includes Cisco CallManager software, and combines an IOS-based multiservice router/voice gateway, application servers running core voice applications, Web-based management, and seamless connectivity to Cisco Catalyst switches.

Cisco Systems also offers four Cisco ICS 7750 voice packages for convenient and cost-effective entry points for customers to deploy IP telephony solutions in their LAN networks. These ICS voice packages are pre-configured to simplify ordering of the necessary voice components including voice mail for a mid-market business or branch site.

When to Sell

Sell This Product	When a Customer Needs These Features
ICS 7750 Integrated Communications System	• A branch office/midmarket business with standalone IP telephony needs from 35-500 users • An end-user customer or partner who wants a single "box" (or platform) IP telephony solution to ease deployment and/or to standardize on voice configurations across multiple sites • An existing multiservice data network customer who wants to add IP telephony functionality to create a converged network solution

Key Features

- Integrated Functionality (includes CallManager for call-processing, multiservice router/voice gateway, Web-based management, and core voice applications)
- Modular chassis architecture features 6 universal slots with hot swapability
- Modular industry-proven Cisco IOS-based Multiservice Route Processor (MRP) delivers data routing and voice trunking; ensures end-to-end QoS
- Industry-leading selection of WAN Interfaces
- World wide selection of voice interfaces
- Optional redundant power supply and uninterruptible power supply
- Optional integrated voice applications including Unity voice/unified messaging, IVR, contact center
- Integrated Web/GUI-based system management tool for simple monitoring and troubleshooting; Console and Telnet access to CLI system management
- Automated inventory, discovery, and configuration of desktop devices and applications
- Automated fault management, auto-notification of problems via e-mail or pager
- Compatible with SNMP-based management tools including CiscoWorks 2000
- N+1 CallManager clustering enables a backup Cisco CallManager to improve system availability

Specifications

Feature	Cisco ICS 7750
System Switch Processor	Fixed slot card; 10/100BaseT autosensing data switch; Two-port RJ-45 connectors; Included with each ICS 7750 system
System Alarm Processor	Fixed slot card; Two serial ports; One console port; Resource Cards; Included with each ICS 7750 system
System Processing Engine	Universal slot card; Intel Pentium III 700 MHz CPU;1 GB SRAM; 40 GB hard disk drive
Multiservice Route Processor	Universal slot card; Standard memory: 64 MB DRAM (max.128 MB); Memory upgrade (option): 16, 32, 64 MB DRAM; Standard flash memory: 16 MB Flash SIMM (max. 80 MB); Flash upgrade (options): 16, 32, 64 MB Flash; modular voice/WAN interface (VWIC) card slots per card; Advanced data networking feature suppot, including: VPN, IPSec 56 and 3DES, Firewall
Dimensions and Weight (HxWxD)	15.75 x 17.25 x 12.5 in. (40.005 x 43.815 x 31.75 cm)Basic configuration-1 MRP, 1 SPE, 1 SSP, 1 SAP (a total of 4 cards = 2 fixed cards + 2 universal cards) and 1 power supply): 42 lb (18.9 kg)
Mounting Options	19 in rack-mount; Standalone

Selected Part Numbers and Ordering Information[1]

Cisco ICS 7750 Voice Packages

ICS-7750-M1V	Cisco ICS 7750 FXO-M1 Analog Voice Package provides eight Foreign Exchange Office (FXO) analog voice interfaces,four analog FXS/DID ports, 25 Cisco Unity Voice Messaging mailboxes and support for upto 50 Cisco CallManager devices.
ICS-7750-TV	Cisco ICS 7750 T1 Digital Voice Package provides 24 digital voice channels (DS0s), 8 analog FXS interfaces, 50 Cisco Unity Voice Messaging mailboxes and support for up to 500 Cisco CallManager devices.
ICS-7750-BV	Cisco ICS 7750 ISDN BRI Voice Package provides four ISDN BRI interfaces(eight B channels), 50 Cisco Unity Voice Messaging mailboxes and support for up to 500 Cisco CallManager devices.
ICS-7750-EV	Cisco ICS 7750 E1 Digital Voice Package provides 30 digital voice channels (DS0s), 50 Cisco Unity Voice Messaging mailboxes and supportfor up to 500 Cisco CallManager devices.

Cisco ICS 77501

ICS-7750	Six-slot ICS chassis, SPE310, SSP, SAP, Power Supply & DOC-CD
SPE310=	System Processing Engine 310 (512MB RAM and Windows 2000)
MRP300=	Multiservice Route Processor 300 with two VIC/WIC slots
MRP3-8FXOM1=	Multiservice Route Processor with 8-ports FXO-M1 and one VIC/WIC slot
MRP3-8FXS=	Multiservice Route Processor with 8-ports FXS and one VIC/WIC slot
MRP3-16FXS=	Multiservice Route Processor with 16-ports FXO-M1
UPS-BASE-UNIT=	UPS with Standard Battery Pack, Ethernet Card (120 V for North America)
UPS-BATT-PACK=	Additional External Battery Pack for UPS Base Unit
PWR-AC-7750=	AC Power Supplyfor ICS 7750 Chassis
FAN-TRAY-7750=	Fan Tray for ICS-7750
ICS-7750-CHASSIS=	ICS-7750 Six-slot chassis & Fan Tray
SAP-7750=	System Alarm Processor for ICS 7750
SSP-7750=	System Switch Processor for ICS 7750

Cisco ICS 7750 WAN Interface Card (WIC) Modules (for MRP cards)

WIC-1DSU-T1=	1-Port T1/Fractional T1 DSU/CSU WAN Interface Card
WIC-1T=	1-Port Serial (T1/E1) Async/Sync WAN Interface Card
WIC-2T=	2-Port Serial (T1/E1)Async/Sync WAN Interface Card
WIC-2A/S=	2-Port low-speed Serial (up to 128kbps) Async/Sync WAN Interface Card spare
WIC-1DSU-56K4=	1-Port 4-Wire 56Kbps DSU/CSU WAN Interface Card
WIC-1B-S/T=	1-Port ISDN BRI S/T WAN Interface Card (dial and leased line)
WIC-1B-U=	1-Port ISDN BRI U with NT-1 WAN Interface Card dial and leased-line

Cisco ICS7750 Voice Interface Card (VIC) Modules (for MRP cards)

VIC-2FXS	Two-port FXS voice/fax interface card
VIC-4FXS/DID	Four-port FXS or DID voice/fax interface card (ports can be configuredfor either FXS or DID)
VIC-2DID	Two-port DID voice/fax interface cad
VIC-2FXO	Two-port FXO voice/fax interface card
VIC-2FXO-M1	Two-port FXO voice/faxinterface cardwith battery reversal and caller ID (for North America)
VIC-2FXO-M2	Two-port FXO voice/faxinterface cardwith battery reversal and caller ID (for Europe)
VIC-2FXO-M3	Two-port FXO voice/faxinterface card with battery reversal and caller ID (for Australia)
VIC-4FXO-M1	Four-port FXO voice/fax interface card withbattery reversal and caller ID (for N. America)
VIC-2E/M	Two-port E&M voice/fax interface cad
VIC-2BRI-NT/TE	Two-port IDSN BRI (NT & TE) voiceinterface card
VWIC-1MFT-T1	One-port T1/fractional T1multiflex trunk with CSU/DSU (for CAS or PRI)
VWIC-2MFT-T1	Dual-port T1/fractional T1multiflex trunk with CSU/DSU (for CAS or PRI)
VWIC-1MFT-E1	One-port E1/fractional E1multiflex trunk with CSU/DSU (for PRI)
VWIC-2MFT-E1	Dual-port E1/fractional E1multiflex trunk with CSU/DSU (for PRI)

Cisco ICS 7750 Packet Voice/Fax DSP Modules (for MRP cards)

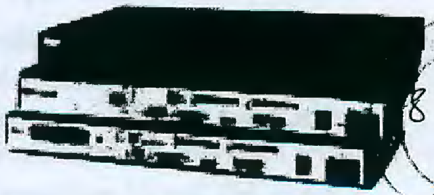
PVDM-256K-4=	4-Channel Packet Voice/Fax DSP Module
PVDM-256K-8=	8-Channel Packet Voice/Fax DSP Module
PVDM-256K-12=	12-Channel Packet Voice/Fax DSP Module
PVDM-256K-16=	16-Channel Packet Voice/Fax DSP Module
PVDM-256K-20=	20-Channel Packet Voice/Fax DSP Module

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the ICS 7750 Web site: **http://www.cisco.com/go/ics7750**

Cisco IAD 2400 Series Integrated Access Device with IOS Telephony Service (ITS)[1]



The Cisco IAD 2400 Series integrated access devices (IADs) combine data, voice, and video services over IP and ATM networks to provide cost-effective and efficient means of delivering high-speed Internet and voice services to small- and medium-sized business customers—all in a small (1 RU) system. When configured with optional ITS software, the IAD 2400 is ideal for delivering converged LAN IP telephony in small office environments (5-20 phones) that do not require CallManager functionality.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco IAD 2400 Series	Business-class, fully integrated accessdevice • IOS Telephony Service (ITS), ideal for small offices (5-20 phones) that donot need Cisco CallManager capabilities • Support for standard phones and IP phones on asingle platform • 8 FXS/16 FXS/16FXS+8FXO analog voice ports and 1 T1 digital voice port models • T1-PPP, FR, HDLC, ATM, ADSL and G.shdsl WAN interfaces

Key Features

- Combines high-speed Internet access and toll-quality voice services on single IOS-based platform (ITS introduced in Cisco IOS Release 12.1(5)YD)
- Offers TDM, VoIP, and VoATM (AAL2) on a single platform
- Seamless migration of customers from TDM-based GR-303 to packet-based GR-303 networks or to call agent-based networks
- Automated remote installation and configuration enabled via Simple Network-enabled Auto Provisioning (SNAP) and the Cisco Configuration Express tool

Competitive Products

- Adtran: TA850, TA750, TA600
- Carrier Access: Adit 600
- Coppercom: MXR 400
- RAD: LA-110, LA-140
- Verilink (formerly Polycom): NetEngine 6200, 7200
- Wave7 Optics: LMG-B

Specifications

Feature	IAD 2421	IAD 2423	IAD 2424
Fixed LAN Ports	1-port Ethernet (10BASE-T)	Same as IAD 2421	Same as IAD 2421
Fixed WAN Ports	1-port T1	1-port ADSL	1-port G.SHDSL
Voice Ports	Analog: 8FXS, 16FXS, 16FXS+8FXO; Digital: 1 T1	Analog: 8FXS	Analog: 8FXS, 16FXS, 16FXS+8FXO; Digital: 1 T1
Processor Speed (type)	80 MHz (RISC)	Same as IAD 2421	Same as IAD 2421
Flash Memory	16 MB (Default); 32 MB (Max)	16 MB (Default); 32 MB (Max)	16 MB (Default);32 MB (Max)
DRAM Memory	64 MB	64 MB	64 MB
Dimensions (HxWxD)	1.7 x 17.5 x 11.3 in.	Same as IAD 2421	Same as IAD 2421

For More Information

See the Cisco IAD 2400 Web site: **http://www.cisco.com/go/2400**

[1] IP Keyswitch capabilities also available with 2600 and 3600 series routers; see IP Keyswitch Web site: http://www.cisco.com/go/keyswitch

Cisco Voice Gateways

Voice Gateways interface directly to PBXs or public telephone networks to carry voice traffic across IP networks—by converting IP calls to standard telephony calls and vice versa. They provide connectivity between packet telephony and legacy telephony such as PSTN, PBX, fax machines, and other devices.

Cisco's full line of multiservice routers can also add analog and digital voice gateway functionality through the use of network modules and voice interface cards[1], such as the Catalyst 6000 Family FXS Analog Interface Module.

Cisco offers the Cisco VG248 dedicated voice gateway.

Cisco VG248 Voice Gateway

The Cisco VG248 Voice Gateway is a 1 unit high rack mountable device allowing 48 analog devices (phones, fax machines & modems) to be used with Cisco Call Manager. It enables organizations with large numbers of analog phones (hotels, universities, hospitals, etc.) to deploy IP Telephony while maintaining the investment in legacy handsets. The analog lines are full featured (caller id, message waiting lights, feature codes) and the price per port is competitive with a legacy PBX.

The VG248 will generate SMDI for the attached analog ports allowing connection to a Cisco Call Manager network through legacy voicemail systems. It shares existing SMDI based voicemail systems between the Cisco Call Manager and the legacy PBX.

Selected Part Numbers and Ordering Information

Cisco VG 248 Voice Gateway

VG248	48 Port Voice over IP analog phone gateway

For More Information

See the Cisco Voice Gateways Web site: **http://www.cisco.com/go/voicegate**

Cisco IP/VC 3500 Series Videoconferencing Products

The IP/VC 3500 series is for enterprises and service providers who want a reliable, easy-to-manage, cost-effective network infrastructure for videoconferencing over their IP networks. They consist of the IP/VC 3511 Multipoint Control Unit (MCU, also known as a "video bridge"), the IP/VC 3521 and 3526 H.320 to H.323 Gateways and the IP/VC 3540-Series Videoconferencing System. The Cisco IP/VC product family works with H.323-standards-based videoconference client devices from a variety of vendors and integrates with legacy H.320 networks.

- The Cisco IP/VC 3511 Multipoint Control Unit (MCU) is a 1RU stack/rack-mount system enabling adhoc videoconferences between three or more endpoints. Multiple participants in multiple locations attend the same meeting with real-time interactivity. It is suitable for small to medium enterprises and remote branch offices in larger enterprises
- The IP/VC 3521 and the IP/VC 3526 Videoconferencing Gateways are also 1RU stack/rack-mount systems that translate between H.320 and H.323 protocols. The IP/VC 3521 provides up to four BRI interfaces and the IP/VC 3526 provides one ISDN T1/E1 PRI interface

[1] Please see the 1700, 2600, 3600, 7200, 5x00 series in Chapter 1—Routers, Chapter 7—Access Products.

- The IP/VC 3540 Videoconferencing System integrates multipoint control units, and gateways I onto a single platform for cost-effective deployment of IP-centric videoconferencing networks. In addition, the IP/VC 3540 platform offers T.120 data conferencing through an optional collaboration server. Customers can add the Rate Matching module which enhances the video composition of any multipoint conference. Enhanced features such as Rate Matching, a number of robust Continuous Presence formats and audio transcoding are available
- The Multimedia Conference Manager (MCM) software is part of Cisco IOS Software and available across a wide range of Cisco router platforms, including the Cisco 2600/2600XM, 3600, 3700, and 7200 series. As a gatekeeper/proxy, it enables network managers to control and secure bandwidth and priority settings for H.323 videoconferencing services

Selected Part Numbers and Ordering Information[1]

Cisco IP/VC 3500 Series Videoconferencing Products

IPVC-3511-MCU	IP/VC 3511 H.323 Videoconference Multipoint Control Unit
IPVC-3521-GW-4B	IP/VC 3521 H.320-H323 VideoconferencingGateway with 4 BRI ports
IPVC-3526-GW-1P	IP/VC 3526 H.320-H.323 Videoconferencing.Gateway-1 PRI
IPVC-3540-MC03A	IP/VC 3540 MCU Module - 30 Sessions - (also available in 60 and 100 session capacities)
IPVC-3540-XAM03	IP/VC 3540 Audio Transcoder for 30 session MCU (also available for 60 session MCU)
IPVC-3540-RM	IP/VC 3540 Rate Matching Module (allowsdifferent ratesin the same conference)
IPVC-3540-GW2P	IP/VC 3540 H.320 to H.323 Gateway Module
IPVC-3540-XAG	IP/VC 3540 Gateway AudioTranscoder
IPVC-3540-AS	IP/VC 3540 ApplicationServer (CPU requiredfor T.120 Data Conferencing Server
IPVC-3540-DS03	IP/VC 3540 T.120 Data Conferencing Server software (also available in 60 sessions)
MCM Images	IP/H323 (Routers: 2600, 3600, 3700)
IOS 12.2(11)T	Enterprise Plus/ H323 MCM (Routers: 2600, 3600, 3700) Enterprise MCM (Routers: 7200)

[1] This is only a small subset of all parts available. Some parts have restricted access or are not available through distribution channels.

For More Information

See the IP/VC 3500 series Web site: **http://www.cisco.com/go/ipvc**

Cisco IP/TV 3.4

Cisco IP/TV® 3.4 delivers a complete, highly scalable, bandwidth-efficient solution for high-quality video communications over enterprise networks. Cisco IP/TV supports live video, scheduled video, video on demand (VOD), synchronized presentations and screen captures, and a wide range of video management functions. The solution enables a broad spect.um of applications for enterprise communications including training, corporate communications, business TV, and distance learning.

Cisco IP/TV 3.4 are purchased as Cisco IP/TV 3400 Series Server appliances or software for third party servers. The Cisco IP/TV 3400 Series servers contain pre-configured software, preinstalled capture cards, network interface cards, and device drivers. The Cisco IP/TV 3400 Series includes the IP/TV 3412 Control Server, the IP/TV 3425 and 3425A Broadcast Servers, the IP/TV 3432 Archive Server, and the IP/TV 3417 Video Starter System. This product family offers a range of choices to best suit large-scale enterprise applications, performance requirements, and bandwidth availability.

Selected Part Numbers and Ordering Information[1]

Cisco IP/TV 3400 Series Video Servers	
IPTV-3412-CTRL	Cisco IP/TV 3412 Control Server
IPTV-3425-BCAST-M	Cisco IP/TV 3425 MPEG-1, MPEG-2 Full D1 Broadcast Server
IPTV-3425A-BCAST-M	Cisco IP/TV 3425 MPEG-1 Broadcast Server
IPTV-3432-ARCH	Cisco IP/TV 3432 Archive Server
IPTV-3417-START-M	Starter Kit
Cisco IP/TV Software	
IPTV-CM-3.4	IP/TV Content Manager
IPTV-SERV-3.4	Broadcast/Archive Server
IPTV-SERV-MP4-3.4	Server w/ MPEG-4 card & license
IPTV-START-HD1-3.4	Starter Kit

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the IP/TV 3400 series Web site: **http://www.cisco.com/go/iptv**

Web Collaboration—Cisco Web Collaboration Option

The Cisco Web Collaboration Option enables businesses to combine the personal value of human interaction with the information value of the Web-creating a powerful environment for driving increased sales, exceptional service, and customer satisfaction.

The Cisco Web Collaboration Option allows you to add "click-for-help" buttons on your Web site that enable customers to interact with your contact center agents over the Web while conducting a voice conversation (PSTN or Voice over IP [VoIP]) or text chat. Contact center agents and callers can share Web pages-including personalized or dynamically generated pages, complete forms in a collaborative fashion, and share any Windows desktop application using nothing more than a Web browser. By facilitating effective, personalized assistance designed to greatly enhance the customer experience, the Cisco Web Collaboration Option is an ideal solution for both sales- and service-oriented contact centers.

The Cisco Web Collaboration Option can be deployed in a pure IP environment or can be seamlessly integrated with your organization's existing telephony infrastructure to provide automated, blended delivery of phone and Web-based inquiries.

Selected Part Numbers and Ordering Information[1]

Cisco IP/TV 3400 Series Video Servers	
CCS-CCSSVR	Cisco Web Collaboration and Media Blender Software

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco Collaboration Server Web site: **http://www.cisco.com/go/ccs**

E-Mail Response Management–Cisco E-mail Manager

Cisco E-Mail Manager is a comprehensive, enterprise-class solution for managing high volumes of customer inquiries submitted to your company mailboxes or Web site. Based on customizable business rules, Cisco E-Mail Manager accelerates the response process by automatically directing messages to the right agent or support team, categorizing and prioritizing messages, suggesting relevant response templates, and, if desired, sending automated replies. A full-featured, browser-based interface provides your agents with the productivity tools and knowledge resources they need to provide fast, accurate and personalized responses to your customers. Cisco E-Mail Manager gives managers the queue management, reporting and outbound marketing tools they need to ensure that desired service standards are met, gain valuable insight into customer needs and generate new revenue opportunities.

Whether you are building a customer support system from the ground up or integrating with existing organizational structures and legacy systems, Cisco E-Mail Manager's uniquely flexible, extensible and scalable design delivers a cost-effective, easy-to-implement strategy for building customer relationships over the Internet.

Selected Part Numbers and Ordering Information[1]

Cisco Email Manager	
CEM-SVR-W	Cisco Email Manager Server (Win 2K)
CEM-AGT	Cisco Email Manager Agent License

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

Cisco Emergency Responder

Cisco Emergency Responder revolutionizes enterprise telephony support for E9-1-1 in North America, E1-1-2 in Europe, and other emergency telephone services across the globe. Traditional PBX E9-1-1 implementations in North America support "automatic location identification" of emergency callers through daily manual database update processes, which limit the frequency of location updates and increase the likelihood of update errors. The Cisco Emergency Responder software application works with Cisco CallManager to automatically track the location of Cisco IP phones in enterprise campuses, route emergency calls to an appropriate public safety answering point (PSAP), and provide the location of the caller to the Public Safety Answering Point (PSAP).

Cisco ER performs these functions without requiring tedious manual database updates after phone moves/adds/changes, which significantly reduces the time, headcount, and costs associated with traditional PBX E9-1-1 maintenance. While some vendors may automate location updates, they still require manual PBX configuration changes to trigger the updates. The Cisco ER solution, when coupled with the automated phone moves/adds/changes features in Cisco CallManager, is the first in the industry to completely automates the phone move process while maintaining E9-1-1 and location data integrity.

In addition, Cisco ER can use email/pager messaging, telephone calls, and auto-refreshing webpage updates to notify on-site security operations personnel and third-party agencies of emergency calls in progress.

Key Features

- Meets and exceeds traditional E9-1-1 requirements
- Automates all user and phone moves, adds, and changes; Enables users and phones to move an unlimited number of times per day
- Avoids the expense and burden of daily PS-ALI record uploads
- Avoids daily error-prone documentation and database updates
- Enables quicker and more effective emergency response from onsite personnel and public agencies
- Provides configuration auditing to facilitate responsible change management and investigative or legal processes
- Provides call history logs for capacity planning, management of emergency call abuse, and incident documentation
- Compatible with any emergency number

Specifications

Feature	Cisco Emergency Responder
Supported Platform	Cisco Media Convergence Server, MCS-7835-1266 and MCS-7825-1133
System Capacity	A single Cisco Emergency Responder server supports 10,000 phones and 30,000 Ethernet switch ports. Additional scalability parameters include 500 Emergency Response Locations (ERLs)- locations that can be uniquely identified to a Public Safety Answering Point (PSAP)- as well as 500 manually entered endpoints such as analog or proprietary phones or H.323 clients. Cisco recommends a second Emergency Responder server to form a fully redundant Cisco Emergency Responder Group with the same capacity and increased availability compared with a single Cisco Emergency Responder server. Larger campuses and distributed systems are supported via a network of Cisco Emergency Responder groups called a Cisco Emergency Responder Cluster
Configurable Elements	
Cisco CallManager	Call routing and digit manipulation to forward user-initiated emergency calls and PSAP return calls to and from Cisco Emergency Responder as appropriate
Cisco Emergency Responder	System administration interface-foraccess to all configuration components or oversight of outsourced vendors LAN administration interface-for IT LAN group or an outsourced vendor Emergency Response Location (ERL) administration interface-for IT telecom group or an outsourced vendor
Other Components	Configure e-mail account on a Simple Mail Transfer Protocol (SMTP) Internet mail server for use by Cisco Emergency Responder Configure an email-to-pager gateway, or use an email paging service Configure a PS-ALI transfer application provided by the PS-ALI database service provider (often requires a dialup modem connection) Provision an E9-1-1 capable voice trunk (Centralized Automated Message Accounting [CAMA] or Primary Rate Interface [PRI]) through a localexchange carrier
Supported Switches[1]	Cisco Catalyst 2950, 3500, 3550, 4000, 4500, 6500 Series

[1] Check for updates on CCO, and following is list of tested switch platforms at time of printing

Selected Part Numbers and Ordering Information[1]

Cisco Emergency Responder

SW-ER1.1-SVR	Cisco Emergency Responder software (MCS platforms), including 100 user licenses
SW-ER1.1-SVR-CPQ=	Cisco Emergency Responder software (Compaq platforms) including 100 user licenses
SW-KEY-ER1.1-USER=	Incremental single-user license key for Cisco Emergency Responder

[1] Redundant user licenses are not required when ordering redundant CER servers for a single CER group.

For More Information

See the Cisco Emergency Responder Web site: **http://www.cisco.com/go/cer**

Cisco ATA Series of Analog Telephone Adaptors

The Cisco ATA 186 and 188 Analog Telephone Adaptors bring analog telephones into the networked world. The Cisco ATA series of products address the low-end product portfolio need by targeting the enterprise, business local services, small-office environment and the emerging managed voice services market. These cost effective handset-to-Ethernet adaptors enable analog devices, such as phones and fax machines, to support voice-over-IP (VoIP) services. The Cisco ATA 186 is equipped with, and a single RJ-45 Ethernet port. The Cisco ATA 188 has two RJ-11 voice ports and two RJ-45 ports. The internal Ethernet switch allows for a direct connection to a 10/100BASE-T Ethernet network and connectivity to a co-located PC or other Ethernet-based device via the RJ-45 ports.

Both models ship with a bootload image and must be upgraded to a signaling firmware image available on Cisco.com before deployment. Cisco ATAs can be configured[1] to use the standards-based Voice over IP (VoIP) protocols H.323, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP) and Skinny Client Control Protocol (SCCP).

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco ATA Series of Analog Telephone Adaptors	• Enable analog devices, such as phones and fax machines, to support Voice over IP services by converting the analog signal into an IP signal • Continue use of existing analog phones with IP network

Key Features

- Auto-provisioning with Trivial File Transfer Protocol (TFTP) provisioning servers
- Automatic assignment of IP address, network route IP, and subnet mask via Dynamic Host Configuration Protocol (DHCP)
- Optional web configuration through built-in Web server
- Optional touch-tone telephone keypad configuration with voice prompt
- Administration password to protect configuration and access
- Advanced pre-processing to optimize full-duplex voice compression
- High performance line-echo cancellation eliminates noise and echo
- Voice activity detection (VAD) and comfort noise generation (CNG) save bandwidth by delivering voice, not silence
- Dynamic network monitoring to reduce jitter artifacts such a packet loss

[1] Two softrware image combinations are available on Cisco.com: H.323/SIP and MGCP/SCCP. MGCP/SCCP image includes the letters, ms, in its name.

Specifications

Feature	Cisco ATA 186	Cisco ATA 188
Telephone and network interfaces	2 RJ-11 FXS ports 1 RJ-45 interface for networkconnection	2 RJ-11 FXS ports 1 RJ-45 interface for networkconnection 1 RJ-45 "switch port" for connectionto PC or another downstream Ethernet port
Dimensions (H x W x D)	1.5 x 6.5 x 5.75 in. (3.8 x 16.5 x14.6 cm)	1.5 x 6.5 x 5.75 in. (3.8 x 16.5 x14.6 cm)
Weights	15 oz (425 gm)	15 oz (425 gm)
Voice-over-IP (VoIP) protocols	H.323 v2; H.323 v4; SIP (RFC 2543); MGCP 1.0 (RFC 2705); MGCP 1.0/network-based call signaling (NCS) 1.0 Profile; MGCP 0.1; SCCP	H.323 v2; H.323 v4; SIP (RFC 2543); MGCP 1.0 (RFC 2705); MGCP 1.0/network-based call signaling (NCS) 1.0 Profile; MGCP 0.1; SCCP

Selected Part Numbers and Ordering Information[1]

Cisco ATA Series of Analog Telephone Adaptors

ATA186-I1	Cisco ATA 186 2-port adaptor, 600 ohm impedance
ATA186-I2	Cisco ATA 186 2-port adaptor, complex impedance (270 ohm in series with 750 ohm and 150 nF in parallel)
ATA188-I1	Cisco ATA 188 2-port adaptor with switch, 600 ohm impedance
ATA188-I2	Cisco ATA 188 2-port adaptor with switch, complex impedance (270 ohm in series with 750 ohm and 150 nF in parallel)

Cisco ATA Series of Analog Telephone Adaptors Power Supply Cables

ATACAB-NA	ATA power suppl cable for North American-style power systems
ATACAB-EU	ATA power suppl cable for Continental European-style power systems
ATACAB-UK	ATA power supply cable for United Kingdom
ATACAB-AR	ATA power suppl cable for Argentina
ATACAB-JP	ATA power suppl cable for Japan

[1] Some countries have telephone networks that list multiple impedance requirements. It is important to closely approximate the impedance of the typical handsets used in the region when selecting the proper configuration. The incorrect choice may lead to poor echo cancellation performance.

For More Information

See the Cisco ATA Series Web site: **http://www.cisco.com/go/ata186**

CHAPTER 5

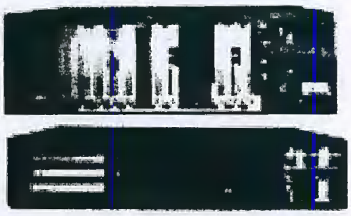
VPN and Security Products

VPN and Security Products at a Glance

Product	Features	Page
Cisco PIX Firewall	Market-leading, purpose-built applianceswhich provide broad range of integrated secuity services • Robust stateful inspection firewalling with applicationawareness • Highly scalable remote access and site-to-site VPN • Intrusion protection with forreal-time responseto network attacks • Award-winning statefulfailover for enterprise-class resiliency	5-2
Cisco IOS Firewall	• Tightly integrated with IOS VPN and advanced routingtechnologies • Stateful packet filteringvia context-based access control(CBAC) • Inline Intrusion detection for realtime response tonetwork attacks • Dynamic, network-to network, per-user authentication and authorization via TACACS+ and RADIUS	5-5
Firewall Blade for Catalyst 6500	Firewall Module is a high performanceintegrated statefulfirewall solutionfor Catalyst 6500 family of switches with performance exceeding 5GB. It is based on proven PIX technology while providing the following benefits to the customers • Investment protection • Low cost of ownership • Ease of use • Operational Consistency • Scalability See the Catalyst 6500 Series Switch in Chapter 2: LAN Switching, page 2-20 , for more information	2-20
Cisco VPN 3000 Family	Remote access Virtual Private Networkplatform • Has models for all size companies, from small to large enterprise organizations • Reduces communications expendtures • Enables users to easily add capacty and throughput	5-6
Cisco IDS Network Sensor	Network-based, real-time intrusion detection system capable of monitoring an entire enterprise network • Distributed intrusion detection system capable of directing andforwarding alams between local, regional, and headquartersbased monitoring consoles • Scalable architecture to allow the depbyment of large numbersof sensors in orderto provide comprehensive security coverage in large networks with performance requirements from T1 to gigabit environments • Cisco IDS Module enablescustomers toperform both securitymonitoring and switching functionswithin the samechassis • CTR (Cisco Threat Response)delivers patented adaptive scan techniques to minimize false alarms	5-8
Cisco Security Agent	The Cisco Security Agent provides threat protection fordesktop andserver computing systems by identifying andpreventing malcious activity. By acting on threats orattacks beforethey can occur, Cisco Security Agent removes known and unknown security risks to enterprise networks and applications: • The Cisco Security Agent aggregates andextends multiple endpoint securityfunctions by providing hostintrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent package • Protects against know andunknown attacks on both servers and desktops	5-10
Cisco 7100 Series	Large branch and centralsite VPN router • Comprehensive suite of VPN services, including encryption, tunneling, firewall, and bandwidth management • Embedded I/O for ease of deployment • Service module slot for IPSec and PPTP encryptioncoprocessing • Dedicated Site-to-Ste VPN router	5-11

Product	Features	Page
Cisco Secure Access Control Server (ACS) for Windows	Controls the authentication, authorization,and accounting (AAA) of users and administrators to network devices and services • Operates as a centralized Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) server • Supports LDAP user authentication • Data replication and backupservices • Flexible user and group policy controls • Support for Cisco802.11x Catalyst Switch and Wireless solutions • Extensible Authentication Protocol (EAP) enhancements to support ProtectedEAP (PEAP) for wireless LANs • All administrative access is encryptedwith SSL	5-14
Cisco Secure User Registration Tool (URT)	Identifiesuserswithinthe network and createsuser registrationpolicybindingsthat help support mobility and tracking: • Ensures that users are associated with their authorized subnet/VLAN • Addresses the challengesassociated with campus user mobility • Supports Web-based authentication for Windows, Macintosh, and Linux client platforms • Secure user accessto the VLAN with MAC address-based security option • Option to allow multiple users connected to a hub to access a VLAN served by a single switch port	5-15
CiscoWorks VPN/Security Management Solution	Combines general device management tools for configuring, monitoring, and troubleshooting enterprise networks with powerful security solutions for managing virtual private networks (VPNs), firewalls, and networkand host-based intrusion detection systems (IDS). This bundle includes: Management and Monitoring Centers, Cisco IDS Host Sensorand Console, Cisco Secure Policy Manager, VPN Monitor, Resource Manager Essentials, and Cisco View See Chapter 9—CiscoIOS Software and Network Management formore informationon CiscoWorks VPN/Security Management Solution	9-16
Cisco 806, 1700, 2600, 3600, 7200, 7400 and SOHO 70 Series	Wide variety of modular router platformswith optionsfor IOS-basedand hardware-enabledVPN and security support. See individual productpagesand Cisco IOS Firewall Feature Set (page 5-5).	1-1

Cisco PIX Firewall Series



The world-leading Cisco PIX® Firewall Series of purpose-built security appliances provides robust, enterprise-class, integrated network security services, including stateful inspection firewalling, virtual private networking (VPN), intrusion protection, and much more-in cost-effective, easy-to-deploy solutions. Ranging from compact, "plug-and-play" desktop firewalls for small and home offices to carrier-class gigabit firewalls for the most demanding enterprise and service-provider environments, Cisco PIX Firewalls provide robust security, performance, and reliability for network environments of all sizes.

When to Sell

Sell This Product	When a Customer Needs These Features
PIX 501	• Small Office / Home Office desktop integrated security appliance • Up to 10 Mbps of firewall throughput and 3Mbps of 3DES VPN throughput[1] • Hardware VPN client (Easy VPN Remote) • VPN concentrator services (EasyVPN Server) for up to 5 remote users • Integrated four pot 10/100 Mbps switch
PIX 506E	• Remote Office / Branch Office desktop integrated security appliance • Up to 20 Mbps of firewall throughput and 16 Mbps of 3DES VPN throughput[1] • Hardware VPN client (Easy VPN Remote) • VPN concentrator services (EasyVPN Server) for up to 25 remote users • Maximum of two 10BASE-T Ethernet interfaces • OSPF dynamic routing support

Sell This Product	When a Customer Needs These Features
PIX 515E	• Small-to-Medium Business (SMB) integrated secuity appliance • Up to 188 Mbps of firewall throughput[1] • Up to 140 Mbps of 3DES/AES-256 VPN throughput[1] using hardware acceleration (integrated inselect models, optional for others) • VPN concentrator services (Easy VPN Server) for up to 2,000 remote users • Up to six 10/100 FE interfaces • VLAN trunking (802.1q tag-based) and OSPF dynamic routing support • Active/standby stateful failover support
PIX 525	• Enterprise-class integrated securty appliance • Up to 330 Mbps of firewall throughput[1] • Up to 155 Mbps of 3DES/AES-256 VPN throughput[1] using hardware acceleration (integrated inselect models, optional for others) • VPN concentrator services (Easy VPN Server) for up to 2,000 remote users • Gigabit Ethernet support; Upto eight 10/100 FE or three Gigabit Ethernet interfaces • VLAN trunking (802.1q tag-based) and OSPF dynamic routing support • Active/standby stateful failover support
PIX 535	• Carrier class large enterprise and service provider firewall appliance • Up to 1.7 Gbps of firewall throughput[1] • Up to 440 Mbps of 3DES/AES-256 VPN throughputusing hardware acceleration (integrated in select models, optional for others) • VPN concentrator services (Easy VPN Server) for up to 2,000 remote users • Gigabit Ethernet throughput; Up to ten 10/100 FE or nine Gigabit Ethernet interfaces • VLAN trunking (802.1q tag-based) and OSPF dynamic routing support • Redundant, hot-swappable power supplies • Active/standby stateful failover support

1. At 1400-byte packets

Key Features

- Security—Purpose-built firewall appliance with a proprietary, hardened operating system
- Performance—Stateful inspection firewall capable of up to 500,000 concurrent connections and 1.7 Gbps of throughput (at 1400-byte packets on Cisco PIX 535 Firewalls)
- High availability—Award-winning, active/standby stateful failover model provides enterprise-class, cost-effective resiliency
- Virtual Private Networking (VPN)—Supports both standards-based IPsec and L2TP/PPTP-based VPN services
- Optional PIX VPN Accelerator Card+—Scales 3DES/AES-256 VPN throughput up to 440 Mbps, using specialized co-processors designed for accelerating encryption operations
- Free software Cisco VPN Client provides secure connectivity across a broad range of platforms including Windows, Mac OS X, Linux and Solaris
- Network Address Translation (NAT) and Port Address Translation (PAT)—Conceals internal IP addresses and expands network address space
- Denial-of-Service (DoS) Attack Protection—Protects the firewall, internal servers and clients from disruptive hacking attempts
- OSPF dynamic routing support for improved network reliability and performance
- VLAN trunking (802.1q tag) support for simplified deployment in switched network environments
- Web-Based PIX Device Manager (PDM)—For simplified configuration and usage reports
- Auto Update, SSH, SNMP, TFTP, HTTPS, and telnet for remote management
- Support from two 10/100 Ethernet interfaces up to nine Gigabit Ethernet interfaces

Competitive Products

- Check Point Software: FireWall-1 / VPN-1
- NetScreen: NetScreen SecurityAppliances
- Nokia: IP-Series SecurityAppliances
- SonicWALL: SonicWALL Security Appliances
- WatchGuard Technologies: Firebox-series and V-series Security Appliances

Specifications

Feature	PIX 501	PIX 506E	PIX 515E	PIX 525	PIX 535
Processor	133 MHz	300 MHz	433 MHz	600 MHz	1.0 GHz
RAM	16 MB	32 MB	32 or 64 MB	128 or 256 MB	512 MB or 1 GB
Flash Memory	8 MB	8 MB	16 MB	16 MB	16 MB
PCI Slots	None	None	2	3	9
Fixed Interfaces (Physical)	Four port 10/100 switch (inside), One 10Base-T Ethernet (outside)	Two 10Base-T Ethernet	Two 10/100 Fast Ethernet	Two 10/100 Fast Ethernet	None
Maximum Interfaces (Physical and Virtual)	Four port 10/100 switch (inside), One 10Base-T Ethernet (outside)	Two 10Base-T Ethernet	Six 10/100 Fast Ethernet (FE) or 8 VLANs	Eight 10/100 FE or GEn or 10 VLANs	Ten-10/100 FE or GE or 24 VLANs
VPN Accelerator Card+ (VAC+) Option	No	No	Yes, integrated in select models	Yes, integrated in select models	Yes, integrated in select models
Failover Support	No	No	Yes, UR/FO models only	Yes, UR/FO models only	Yes, UR/FO models only
Size	Desktop	Desktop	1 RU	2 RU	3 RU

Selected Part Numbers and Ordering Information[1]

Cisco PIX Bundles	
PIX-535-UR-BUN	PIX 535 Unrestricted Bundle (Chassis, unrestricted license, two 10/100 ports, VPN Accelerator Card+)
PIX-535-R-BUN	PIX 535 Restricted Bundle (Chassis, restricted license, two 10/100 ports)
PIX-535-FO-BUN	PIX 535 Failover Bundle (Chassis,failover license,two 10/100 ports, VPN Accelerator Card+)
PIX-525-UR-BUN	PIX 525 Unrestricted Bundle (Chassis, unrestricted software, two 10/100 ports, VPN Accelerator Card+)
PIX-525-R-BUN	PIX 525 Restricted Bundle(Chassis, restricted software,two 10/100 ports)
PIX-525-FO-BUN	PIX 525 Failover Bundle (Chassis,failover software, two 10/100 ports, VPN Accelerator Card+)
PIX-515E-UR-BUN	PIX 515E Unrestricted Bundle(Chassis, unrestricted software, two 10/100 ports, VPN Accelerator Card+)
PIX-515E-R-BUN	PIX 515E Restricted Bundle (Chassis, restricted software,two 10/100 ports)
PIX-515E-FO-BUN	PIX 515E Failover Bundle(Chassis, failover software, two 10/100 ports, VPN Accelerator Card+)
PIX-506E-506E-BUN-K9	PIX 506E 3DES/AES Bundle (Chassis, software, 3DES/AES license, two 10-BaseT ports)[2]
PIX-501-BUN-K8	PIX 501 10 User/DES Bundle (Chassis, SW, 10 user/DES licenses, 4 port 10/100 switch)
PIX-501-BUN-K9	PIX 501 10 User/3DES/AES Bundle (Chassis, SW, 10 user/3DES/AES licenses, 4 port 10/100 switch)[2]
PIX-501-50-BUN-K8	PIX 501 50 User/DES Bundle (Chassis, SW, 50 user/DES licenses, 4 port 10/100 switch)
PIX-501-50-BUN-K9	PIX 501 50 User/3ES/AES Bundle (Chassis, SW, 50 user/3DES/AES licenses, 4 port 10/100 switch)[2]
Cisco PIX Interfaces and Cards	
PIX-1GE-66	Single 66-MHz Gigabit Ethernet interface for PIX 53x (multimode fiber, SC connector)
PIX-1GE	Single Gigabit Ethernet Interface for PIX 52x
PIX-4FE	Four-port 10/100 Fast Ethernet interface
PIX-1FE	Single-port 10/100 Fast Ethernet interface
PIX-VPN-ACCEL	IPSec Hardware VPN Accelerator Card (VAC)
PIX-VPN-ACCEL-PLUS	PIX VPN Accelerator Card+ (VAC+)
Cisco PIX VPN Feature Licenses	
PIX-VPN-3DES	3DES/AES IPSec VPN software license for PIX 525/535[2]
PIX-515-VPN-3DES	3DES/AES IPsec VPN software license for PIX 515/515E[2]
PIX-506-SW-3DES	3DES/AES IPSec VPN software license for PIX 506/506E[2]
PIX-501-VPN-3DES	3DES/AES IPSec VPN software license for PIX501[2]
PIX-VPN-DES	56-bit DES IPSec VPN software license
PIX Accessories	
PIX-506E-PWR-AC	Redundant AC power supply for PIX 506E
PIX-515-PWR-DC	Redundant DC power supply for PIX515/515E

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

[2] AES encryption available with Cisco PIX Firewall Software version 6.3 and above.

For More Information

See the PIX Firewall Web site: **http://www.cisco.com/go/pix**

Cisco IOS Firewall

The Cisco IOS Firewall enriches Cisco IOS Software security capabilities, integrating robust firewall functionality and intrusion detection for every network perimeter. When combined with Cisco IOS IPSec software and other Cisco IOS Software-based technologies such as L2TP tunneling and quality of service (QoS), it provides a complete, integrated virtual private network solution. Because it is available for a wide range of Cisco routers, it gives customers the flexibility to choose a solution that meets their bandwidth, LAN/WAN density, and multiservice requirements, while benefiting from advanced security.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco IOS Firewall	• An integrated firewall solution with powerful security and multiprotocol routing al on the same platform • Scalability options from the Cisco 800 up to the Cisco7500 and the Catalyst 6000 • Low cost solution where high performance is not a requirement • For secure extranet and intranet perimeters and Internet connectivity for branch and remote offices • Secure remote access or data transfer via a Cisco IOS Software-based VPN solution • Real-time (inline) integrated intrusion detection system (IDS) to complement firewall or existing IDS (Cisco Secure IDS) • Security and access to the network on a per-user basis

Key Features

- Context-based access control (CBAC) provides secure, stateful, application-based filtering, supporting the latest protocols and advanced applications
- Intrusion detection for real-time inline monitoring, interception, and response to network misuse
- Dynamic, per-user authentication/authorization for LAN, WAN, and VPN clients
- Graphical configuration and management via the ConfigMaker Security Wizard and Cisco Secure Policy Manager (CSPM)
- Provides strong perimeter security for a complete Cisco IOS Software-based VPN solution, including IPSec, QoS, and tunnelling for a wide range of Cisco routers

Competitive Products

- Lucent (Ascend):SecureAccess Firewall
- Nokia: IP400 Series
- Nortel: BaySecure Firewall-1
- Same competitorsas PIX so theyare also Checkpoint, Linksys, Nokia, Netscreen, etc.

Specifications

Feature	Cisco IOS Firewall
Supported Network Interfaces	All network interfaces on supported platforms
Supported Platforms	Cisco 1720, 2600/2600XM, 3600, 7100, and 7200 series router platforms (supports full feature set) Cisco 800, UBR900, 1600, and 2500 series router platforms include all firewall features with exception ofintrusion detection and authenticatin proxy
Simultaneous Sessions	No maximum; dependenton platform, network connection, and traffic

Part Numbers and Ordering Information

For Cisco IOS Images containingfirewall (FW) and intrusion detection (IDS) capabilties, see individual product pagesof supported platforms and the Cisco IOS Feature Navigator at http://www.cisco.com/go/fn (CCO login required) forpart numbers and more info.

For More Information

See the Cisco IOS Firewall Feature Set Web site: **http://www.cisco.com/go/csis**

Cisco VPN 3000 Family

The Cisco VPN 3000 Concentrator Series—A family of purpose-built, remote access Virtual Private Network (VPN) platforms that incorporates high availability, high performance and scalability with the most advanced encryption and authentication techniques available today. Customers can greatly reduce costs by leveraging their ISPs' infrastructure and eliminate costly leased lines. This series supports small offices as well as large organizations with up to 10,000 simultaneous remote users per unit. With load balancing configured, multiple units can be clustered to enable unlimited remote access users. It also supports the widest range of VPN clients including Certicom MovianVPN client, Microsoft 2000 L2TP/IPsec Client, and Microsoft PPTP for Windows 95/98/ME/NT/2000/XP.

The Cisco VPN 3002 Hardware Client—Combines the best capabilities of a software client with the reliability and stability of a dedicated hardware platform, and scales to tens of thousands of users. It sets up connections to a variety of Cisco VPN concentrators, including the VPN 3000 series and PIX firewalls.

When to Sell

Sell This Product	When a Customer Needs These Features
VPN 3005 and 3015 Concentrators	• A fixed configuration device designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous remote access sessions • Encryption processing is performed in software • VPN 3015 is field-upgradable to the Cisco VPN 3030 and 3060 models and for redundancy
VPN 3030 and 3060 Concentrators	• VPN 3030 is for medium- to large-sized organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps max. performance) and up to 1500 simultaneous sessions; field-upgradeable to the Cisco VPN 3060 • VPN 3060 is for large organizations, with high-perfomance, high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps max. performance) and up to 5000 simultaneous remote access sessions • Both have specialized SEP modules to perform hardware-based acceleration
VPN 3080 Concentrator	• Optimized to support large enterprise organizations that demand the highest level of performance combined with support for up to 10,000 simultaneous remote access sessions • Specialized SEP modules perform hardware-based acceleration
VPN 3000 Client	• Establishes secure, end-to-end encrypted tunnels to the Cisco VPN 3000 Concentrator and other Cisco Easy VPN compliant devices. • Provided at no charge, installs on PCs and is available for Windows, MAC OS X and Linux/Solaris environments
VPN 3002 Hardware Client	• Emulates the software client in hardware • Ideal for mixed operating system environments and where corporation does not own/control remote PC or for very large applications requiring large number of devices due to ease of deployment, upgradability & scalability

Key Features

- Cisco VPN 3000 Concentrators Series
  - Support for industry standard IPSec DES/3DES/AES and Cisco IPSec/NAT for VPN Access through Port Address Translation firewalls
  - Unlimited-use license for Cisco VPN Client distribution included at no cost with multiple OS support including Windows, MAC OS X, Linux and Solaris; also integrates with Zone Alarms personal firewall
  - Supports standard authentication: RADIUS, SDI Tokens, and Digital Certificates
  - VPN load balancing allows for multiple units to cluster as a single shared pool
- Cisco VPN 3002 Hardware Client supports up to 253 users/stations per VPN 3002
  - Works with most operating systems including Windows, Linux, Solaris, and MAC OS X
  - Auto-upgrade capability automates upgrades with no user intervention required
  - Client technology employs push policy and automatic address assignment from the central site concentrator, enabling virtually unlimited scalability

Competitive Products

- Nortel: Contivity products
- Netscreen: LAN to LAN environments
- Nokia

Specifications

Cisco VPN 3000 Series Concentrators

Feature	VPN 3005	VPN 3015	VPN 3030	VPN 3060	VPN 3080
Simultaneous Users	100	100	1500	5000	10,000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	No	No	Optional	Optional	Yes
Expansion Slots	0	4	3	2	N/A
Upgradeable	No	Yes	Yes	N/A	N/A
Memory	32 MB	128 MB	128 MB	256 MB	256 MB
Hardware Configuration	1U, Fixed	2U, Scalable	2U, Scalable	2U, Scalable	2U
Power Supply	Single	Single, with a dual option	Single, with a dual option	Single, with a dual option	Dual
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
LAN-to-LAN Connections (internal user database)	100	100	500	1000	1000
Dimensions (HxWXD)	1.75 x 17.5 x 11.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.

Cisco VPN 3002 Hardware Client

Feature	VPN 3002 Hardware Client
Hardware Processor	Motorola PowerPC processor; Dual flash image architecture
Network Interfaces	CPVN3002-K9: One Public 10/100Mbps RJ-45 Ethemet Interface and One Private Port 10/100Mbps RJ-45 Ethernet Interface CVPN3002-8E-K9: One Public 10/100Mbps RJ-45 Ethernet Interface and Eight Private Port 10/100Mbps RJ-45 Ethernet Interfaces via AUTO-MDIX switch
Physical Dimensions	1.967 x 8.6 x 6.5 in. (5 x 8.6 x 16.51 cm)
Power Supply	External AC Operation: 100-240V at 50/60 Hz with universal power factor correction; 4foot cord included and international "pigtail" power cord selection
Tunneling Protocol Support	IPsec with IKE keymanagement
Monitoring & Configuration	Event logging; SNMP MIB-II support Embedded management interface is accessible via console port or local web browser; SSH/SSL
Encryption Algorithms, Key Management & Authentication Algorithms	56-bit DES (IPsec); 168-bit Triple DES (IPsec); AES 128 & 256-bit (IPsec)
Authentication and Accounting Servers	Support for redundant externalauthentication servers including RADIUS Microsoft NT Domain authentication, X.509v3 Digital Certs (PKC7-PKCS10)
Configuration Modes	Client Mode—acts as client, receives random IP address from Concentrator Pool; Uses NAPT to hide stations 3002; Network behind 3002 is unroutable; few configurationparameters Network Extension Mode—acts as site-to-site device; Uses NAPT to hide stations only to Internet (stations visible to central site); Network behind 3002 is routable; additional configuration parameters

Selected Part Numbers and Ordering Information[1]

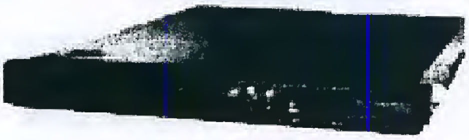
Cisco VPN 3000 Concentrator	
CVPN3005-E/FE-BUN	CVPN3005-E/FE hw set, sw, client, & US power cord
CVPN3015-NR-BUN	CVPN3015-NR non-redundanthw set, sw, client, & US powercord
CVPN3030-NR-BUN	CVPN3030-NR non-redundanthw set, sw, client, & US powercord
CVPN3030-RED-BUN	CVPN3030-RED redundanthw set, sw, client, & US power cord
CVPN3060-NR-BUN	CVPN3060-NR non-redundanthw set, sw, client, & US powercord
CVPN3060-RED-BUN	CVPN3060-RED redundant hwset, sw, client, & US power cord
CVPN3080-RED-BUN	CVPN3080-RED redundant hwset, sw, client, & US power cord
Cisco VPN 3000 Series Upgrades	
CVPN1530-UPG-RED	Cisco VPN 3015 To 3030 (Redundant) Upgrade Kit
CVPN1560-UPG-NR	Cisco VPN 3015 To 3060 (Non-Redundant) UpgradeKit
CVPN1560-UPG-RED	Cisco VPN 3015 To 3060 (Redundant) Upgrade Kit
CVPN1580-UPG-RED	Cisco VPN 3015 To 3080 (Redundant) Upgrade Kit
CVPN3030-UPG-RED	Cisco VPN 3030 To 3080 (Redundant) Upgrade Kit
CVPN3060-UPG-NR	Cisco VPN 3030 To 3060 (Non-Redundant) UpgradeKit

CVPN3080-UPG-R/R	Cisco VPN 3030 (Redundant) to 3080 (Redundant)Upgrade Kit
CVPN3080-UPG-RED	Cisco VPN 3030 To 3080 (Redundant) UpgradeKit
CVPN3060-UPG-RED	Cisco VPN 3030 To 3060 (Redundant) Upgrade Kit
CVPN6060-UPG-RED	Cisco VPN 3060 To 3060 (Redundant) UpgradeKit
CVPN6080-UPG-RED	Cisco VPN 3060 To 3080 (Redundant) UpgradeKit
CVPN3060-UPG-R/R	Cisco VPN 3030 (Redundant) to 3060 (Redundant)Upgrade Kit
CVPN6080-UPG-R/R	Cisco VPN 3060 (Redundant) to 3080 (Redundant)Upgrade Kit
Cisco VPN 3000 Series Accessories	
CVPN3000-PWR=	Cisco VPN 3000 Concentrator Power Supply
Cisco VPN 3000 Series Basic Maintenance	
CON-SNT-PKG4	SMARTnet Maintenance for Cisco CVPN3005-E/FE-BUN
CON-SNT-PKG8	SMARTnet Maintenance for Osco CVPN3015-NR-BUN
CON-SNT-PKG11	SMARTnet Maintenance for Osco CVPN3030-NR-BUN
CON-SNT-PKG13	SMARTnet Maintenance for Osco CVPN3030-RED-BUN
CON-SNT-PKG14	SMARTnet Maintenance for Osco CVPN3060-RED-BUN
Cisco VPN Client	
CVPN-CLIENT-K9=	Cisco VPN Client CD (included with Concentratorpurchase)

For More Information

See the Cisco VPN 3000 series Web site: **http://www.cisco.com/go/vpn3000**

Cisco Intrusion Detection System Network Sensors



Cisco integrated network security solutions enable organizations to protect productivity gains and reduce operating costs. The Cisco Intrusion Protection is designed to efficiently protect your data and information infrastructure. Cisco delivers four four critical elements for efficient intrusion protection system which are:

- Accurate threat detection—Cisco Intrusion Detection System Version 4.0 (Cisco IDS 4.0) delivers the first step in providing a secure environment by comprehensively detecting all potential threats
- Intelligent threat investigation—Cisco Threat Response technology virtually eliminates false alarms, and automatically determines which threats need immediate attention to avoid costly intrusions.
- Ease of management—Browser-based tools simplify the user interaction, while providing powerful analytical tools that allow for a rapid and efficient response to threats.
- Flexible deployment options—A range of high-availability devices provide the flexible backbone for creating the secure and efficient intrusion protection system.

The current Cisco IDS sensing portfolio includes the following sensor appliances: IDS 4210, IDS 4235, IDS 4250, and IDS 4250-XL. Additionally, Cisco IDS delivers network protecting that is integrated into the Catalyst 6500 switch with the Intrusion Detection System Module (IDSM-2).

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco IDS Network Sensors	• Cisco network IDS appliances are network-based, real-time intrusion detection systems capable of monitoring an entire enterpise network • Performance requirements from 45 Mbps to 1 Gbps • The Cisco IDS Module enables customers to perform both security monitoring and switching functions within the same chassis • A robust, 24 hour x 7 day-a-week monitoring and response system with the latest attack detection capabilities • A distributed intrusion detection system capable of directing and forwarding alarms between local, regional, and headquarters-based monitoring consoles • A scalable architecture to allow the deployment of large numbers of sensors in order to provide comprehensive security coverage in large network environments. • An intrusion detection system designed to integrate smoothly with existing network management tools and practices • Automated false alarm reduction capabilities • Integration of fullfeatured IDS protection into the Cisco Catalyst 6500 chassis

Key Features

- High-Speed Performance including support for full line rate gigabit environments
- Easy Installation and Setup; Remote Configuration Capability
- Fault-Tolerant Communications
- Comprehensive Attack Database
- Custom User-Defined Signatures; Automatic Signature Updates
- Notification actions
- Ability to Monitor 802.1q (trunked) traffic
- Secure web-based embedded device management and event monitoring
- Comprehensive IDS Anti-Evasion Techniques
- Cisco IOS-like CLI for full featured IDS management capabilities

Competitive Products

- Internet Security Systems (ISS): RealSecure
- Symantec: Recourse Manhunt & ManTrap/NetProwler
- Enterasys: Dragon IDS
- Intrusion.com: SecureNet
- Snort: IDS
- Tipping Point
- nCircle
- Network Flight Recorder, Inc.: NFR

Specifications

Feature	IDS-4210	IDS-4235	IDS-4250	IDS-4250-XL	IDS Module (IDSM-2)
Performance	45 Mbps	200 Mbps	500 Mbps	1000 Mbps	600 Mbps
Processor	566 MHz	1.26 GHz	Dual 1.26 GHz	Dual 1.26 GHz. Includes customized HW acceleration	Custom Hardware
RAM	256 MB	1 GB	2 GB	2 GB	
Network Interface Card	Autosensing 10/100 Base-T Ethernet	Autosensing 10/100/1000 Base-T Ethernet	Autosensing 10/100/1000BASE-TX with optional 1000-Base SX (fiber)	Dual 1000BASE-SX interface with MTRJ	PCI
Command & Control Interface	Autosensing 10/100 Base-T Ethernet	Autosensing 10/100/1000Base-TX	Autosensing 10/100/1000Base-TX	Autosensing 10/100/1000Base-TX	PCI

Selected Part Numbers and Ordering Information[1]

Cisco IDS Network Appliance Sensor

IDS-4210-K9	4210 Sensor (Chassis, s/w, two 10/100 ports, up to 45Mbps)
IDS-4235-K9	Cisco IDS 4235 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector, up to 200 Mbps)
IDS-4250-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector, upto 500 Mbps)
IDS-4250-XL-K9	Cisco IDS 4250-XL Sensor (chassis, software, SSH, hardware accelerator with dual 1000BASE-SX and MTRJ connectors)

Cisco IDS Switch Sensor Options

WS-SVC-IDS2-BUN-K9	Intrusion Detection System Module for Catalyst 6K Switch (IDSM-2)

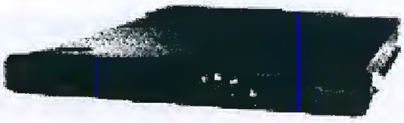
1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

Note **Export Considerations:** The Cisco IDS 4210, Cisco IDS 4235, Cisco IDS 4250, Cisco IDS 4250-XL and Cisco IDSM-2 are subject to export controls. Please refer to the export compliance Web site at **http://www.cisco.com/wwl/export/crypto** for guidance. For specific export questions, please contact **export@cisco.com**.

For More Information

See the Cisco IDS Web site: **http://www.cisco.com/go/ids**

Cisco Security Agent



The next-generation Cisco Security Agent network security software provides threat protection for server and desktop computing systems, also known as "endpoints." The Cisco Security Agent goes beyond conventional host and desktop security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown ("Day Zero") security risks that threaten enterprise networks and applications. The Cisco Security Agent aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent package.

The Cisco Security Agent analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs. Customers require robust endpoint security that prevents security attacks from affecting the network and critical applications.

As a key component of the SAFE blueprint for secure e-business, the Cisco Security Agent provides unprecedented endpoint protection that enables businesses to participate in e-commerce securely and take advantage of the Internet economy.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Security Agent	• Host intrusion protection, distributed firewall, malicious mobile code protection,operating system hardening,file integrity and/or audit logconsolidation. The Cisco Security Agentprovides all of these features in one integrated package • Protection against bothknown and unknown attacks • Protection for servers and/or desktops/laptops • A solution that isscalable to protectthousands of servers and desktopsfor large enterprise deployments

Key Features

- Provides industry-leading protection for Unix and Windows servers
- Open, extensible architecture offers the capability to define and enforce security according to corporate policy

Competitive Products

- Internet Security Systems (ISS)
- Symantec: Intruder Alert
- Enterasys: Squire
- Entercept
- NFR (Centrax)

Specifications

Feature	Cisco Security Server Agent	Cisco Security Desktop Agent	Cisco Security Agent Manager
Platforms	Windows 2000 Server and Advanced Server (up to Service Pack 3) Windows NT v4.0 Server and Enterprise Server (Service Pack 5 or later) Solaris 8 SPARC architecture (64-bit kernel)	Windows NT v4.0 Workstation (Service Pack 5 or later) Windows 2000 Professional (up to Service Pack 3) Windows XP Professional (up to Service 1)	Microsoft Windows 2000 Server and Advanced Server (up to SP 2)

Selected Part Numbers and Ordering Information[1]

Cisco Security Agent Options

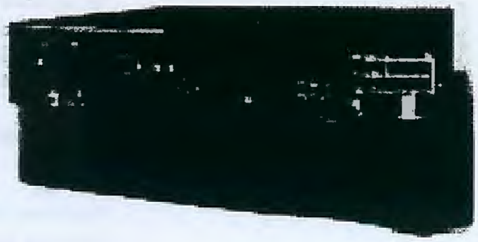
CSA-MANAGER-K9	Cisco Security Agent Manager (CD Kit)
CSA-SRVR-K9=	Cisco Security Server Agent (Win & Sol), 1 Agent
CSA-B10-SRVR-K9	Cisco Security Server Agent (Win & Sol), 10 Agent Bundle
CSA-B25-DTOP-K9	Cisco Security Desktop Agent, 25 Agent Bundle
CSA-B100-DTOP-K9	Cisco Security Desktop Agent, 100 Agent Bundle

Note **Export Considerations:** The Cisco Security Agent is subject to export controls. Please refer to the export compliance Web site at **http://www.cisco.com/wwl/export/crypto** for guidance. For specific export questions, please contact **export@cisco.com**.

For More Information

See the Cisco Security Agent Web site: **http://www.cisco.com/go/securityagent**

Cisco 7100 Series



The Cisco 7100 series VPN router is a high-end, integrated VPN solution that melds high-speed, industry-leading routing with a comprehensive suite of advanced site-to-site VPN services. The Cisco 7100 series VPN router integrates key features of VPNs—tunneling, data encryption, security, firewall, advanced bandwidth management, and service-level validation—to deliver self-healing, self-defending, VPN platforms that cost-effectively accommodate remote-office and extranet connectivity using public data networks. The Cisco 7100 series VPN router offers specific hardware configurations optimized for VPN applications and network topologies. Optional WAN and embedded Fast Ethernet interfaces combined with high-performance routing and rich VPN services provide turnkey VPN routing solutions.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7120	• Entry-level Cisco 7100 Series Router designed for large branch or centralsite VPN with VPN services throughput of up to 50 Mbps • Designed primarily for site-to-site VPN deployments with incidental remote access requirements
Cisco 7140	• High-end site-to-site VPN platform for central site VPN applications with VPN services throughput up to 140 Mbps • Provides superior routing and VPN services performance for central site environments, as well as dual power supplies for increased solution reliability

Key Features

- Comprehensive suite of VPN services—tunneling, data encryption, security, firewall, quality of service, and service level validation—integrated with industry leading routing
- High performance RISC processor delivering high-speed, scalable VPN services and routing throughput and extensive memory for reliable, high-speed VPN services delivery
- Dual autosensing 10/100BASE-T Fast Ethernet ports for connectivity to the corporate LAN; the Cisco 7120 Series also has an integrated 4-port T1/E1 serial WAN interface
- Integrated Services Module (ISM) is included for support up to 2000 simultaneous tunneling sessions with 90 Mbps encryption performance and Windows 95/98/NT4.0 and Windows 2000 compatibility for remote access; an optional Integrated Services Adapter (ISA) may be installed in the Cisco 7140 to provide dual encryption acceleration performance up to 3000 tunnels and 140 Mbps 3DES encryption throughput

Competitive Products

- Check Point: VPN-1 Appliance
- Nortel: Contivity 4500
- Nokia: IP440

Specifications

Feature	Cisco 7120	Cisco 7140
Embedded Dual 10/100BASE-T Fast Ethernet Interfaces	Autosensing, RJ-45	Autosensing, RJ-45
WAN Physical Interfaces	EIA/TIA-232, EIA/TIA-449, X.21, V.35, EIA-530	None
WAN/LAN Interface Expansion Slot	1 slot	1 slot
Supported Network and Services Port Adapters	Gigabit Ethernet 1000BASE-SX and 1000BASE-LX/LH Fast Ethernet 100BASE-TX and 100BASE-FX Fast Ethernet/ISL TX and ISL FX Ethernet 10BASE-T and 10BASE-FL Dedicated Token Ring Multichannel T1 and E1 ATM Synchronous Serial HSSI ISDN BRI Packet over SONET OS3/STM1 Integrated Services Adapter (ISA)	Same as Cisco 7120
Service Module Slot	1 slot	1 slot
Included Service Modules	Integrated Services Module (ISM)	Integrated Services Module (ISM)
Console and Auxiliary Ports	1 of each, RJ-45 interface	1 of each, RJ-45interface
SDRAM	64 MB packet 128 MB system (expandableto 256 MB)	64 MB packet 128 MB system (expandableto 256 MB)
Flash Memory	48 MB	48 MB
PCMCIA Slots for Flash Memory	2	2
Power Supply	Single AC	Dual AC
Dimensions (HxWxD)	3.5 in. x 17.5 in. x 18.25 in.	3.5 in. x 17.5 in. x 18.25 in.

Cisco IOS Software and Memory Requirements[1]

To run the Cisco IOS Software Feature Packs, you need, at a minimum, the amount of memory shown in the following table. Some configurations will require more than the recommended minimum.

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required	DRAM Memory Required
CD71-CL-12.1.6E=	IP IPSEC 56	12.1(6)E	16MB	64MB
CD71-CK2-12.1.6E=	IP IPSEC 3DES	12.1(6)E	16MB	64MB
CD71-CHK2-12.1.6E=	IP/FW/IDS IPSEC 3DES	12.1(6)E	16MB	64MB
CD71-AL-12.1.6E=	Enterprise IPSEC 56	12.1(6)E	16MB	64MB
CD71-AK2-12.1.6E=	Enterprise IPSEC 3DES	12.1(6)E	16MB	64MB
CD71-AHK2-12.1.6E=	Enterprise/FW/IDS IPSEC 3DES	12.1(6)E	16MB	64MB

[1] For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information". For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

Selected Part Numbers and Ordering Information[1]

Cisco 7100 Series Bundles—7120	
CISCO7120-4T1/VPN	7120-4T1 VPN Bundle, ISM, 2xFE, AC PS, IPSEC DES
C7120-4T1/VPN/K9	7120-4T1 VPN Bundle, ISM, 2xFE, AC PS, IPSEC 3DES
Cisco 7100 Series Bundles—7140	
CISCO7140-2FE/VPN	7140-2FE VPN Bundle, ISM, 2xFE, 2xAC PS, IPSEC DES
C7140-2FE/2VPN/K8	7140-2FE VPN Bundle, ISM & ISA, 2xFE, 2xAC PS, IPSEC DES
C7140-2FE/2VPN/K9	7140-2FE VPN Bundle, ISM & ISA, 2xFE, 2xAC PS, IPSEC 3DES
C7140-2FE/VPN/K9	7140-2FE VPN Bundle, ISM, 2xFE, 2xAC PS, IPSEC 3DES
Cisco 7100 Port Adapters	
PA-FE-TX	1-port Fast Ethernet 100BaseTx Port Adapter
PA-FE-FX	1-port Fast Ethernet 100BaseFx Port Adapter
PA-2FE-TX	2-port Fast Ethernet100BaseTx Port Adapter
PA-2FE-FX	2-port Fast Ethernet 100BaseFx Port Adapter
PA-2FEISL-TX	2-port Token Ring ISL 100BaseTx Port Adapter
PA-2FEISL-FX	2-port Token Ring ISL 100BaseFx Port Adapter
PA-4E	4-port Ethernet 10BaseT Port Adapter
PA-8E	8-port Ethernet 10BaseT Port Adapter
PA-5EFL	5-port Ethernet 10BaseFL Port Adapter
PA-4T+	4-port Serial Port Adapter, Enhanced
PA-8T-V35	8-port Serial, V.35 Port Adapter
PA-8T-232	8-port Serial, 232 Port Adapter
PA-8T-X21	8-port Serial, X.21 Port Adapter
PA-4R-DTR	4-port Dedicated Token Ring, 4/16Mbps, HDX/FDX Port Adapter
PA-GE	Gigabit Ethernet Port Adapter
PA-H	1-port HSSI Port Adapter
PA-2H	2-port HSSI Port Adapter
PA-A3-T3	1-port ATM Enhanced DS3 Port Adapter
PA-A3-E3	1-port ATM Enhanced E3 Port Adapter
PA-A3-OC3MM	1-port ATM Enhanced OC3c/STM1 Multimode Port Adapter
PA-A3-OC3SMI	1-port ATM Enhanced OC3c/STM1 Single mode (IR) Port Adapter
PA-A3-OC3SML	1-port ATM Enhanced OC3c/STM1 Single mode (LR) Port Adapter
PA-4E1G/75	4-port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
PA-4E1G/120	4-port E1 G.703 Serial Port Adapter (120ohm/Balanced)
PA-E3	1-port E3 Serial Port Adapter with E3 DSU
PA-2E3	2-port E3 Serial Port Adapter with E3DSUs
PA-T3	1-port T3 Serial Port Adapter with T3 DSUs
PA-2T3	2-port T3 Serial Port Adapter with T3DSUs
PA-MC-2T1	2-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-2E1/120	2-port multichannelE1 port adapterwith G.703 120ohm interf
PA-MC-4T1	4-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-8T1	8-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-8E1/120	8-port multichannelE1 port adapterwith G.703 120ohm interf
PA-POS-OC3MM	1-port Packet/SONET OC3c/STM1 Multimode Port Adapter
PA-POS-OC3SMI	1-port Packet/SONET OC3c/STM1 Single mode (IR) Port Adapter
PA-POS-OC3SML	1-port Packet/SONET OC3c/STM1 Single mode (LR) Port Adapter
SM-ISM	Integrated Services Module for IPSec & MPPE encryption
SA-ISA	Integrated Services Adapter for IPSec or MPPE encryption

PA-4B-U	4-port BRI Port Adapter, U Interface
PA-8B-S/T	8-port BRI Port Adapter, S/T Interface

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 7100 series Web site: **http://www.cisco.com/go/7100**

Cisco Secure Access Control Server for Windows

Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) server system. Cisco Secure ACS controls the authentication, authorization, and accounting (AAA) of users and administrators accessing corporate resources through the network. Cisco Secure ACS greatly reduces the administrative and management burden involved in scaling user and network administrative access to your network. Cisco Secure ACS centralizes the administration of user access controls globally to ensure enforcement of assigned policies.

ACS 3.1 provides support for the latest security architecture for Wireless authentication. It also includes SSL server authentication and encryption for administrative login.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Secure Access Control Server (ACS) for Windows	• Centrally manage who can log in to the network from wired or wireless connections • Privileges each user has in the network • Accounting information recorded in terms of security audits or account billing • What access and command controls are enabled for each configuration administrator • Virtual VSA for Aironet rekey • Secure server authentication and encryption • Simplified firewall access and control through Dynamic Port Assignment • Same User AAA services

Key Features

- PEAP support—Provides a new, secure client-server authentication method for wireless networks; Provides new support for one-time token authentication, password change/aging and powerful extensibility of end-user databases such as LDAP, NDS, and ODBC.
- SSL support for administrative access—Administrative access via the Web GUI can be secured with SSL, both certificate-based and encrypted tunnel support
- CHPASS improvements—Allows privileged users control over whether network administrators can change passwords during TACACS+ AAA client-hosted Telnet sessions
- Improved IP pool addressing mechanism—Includes a new, efficient algorithm for allocating IP addresses
- Device search mechanism—Allows users to search for a configured AAA device based on the device name, IP address, type (RADIUS or TACACS+), or device group
- Improved PKI support—Provides a more secure PKI authentication scheme by verifying the user's certificate authority stored in the remote LDAP directory against the one provided by the client

- EAP proxy enhancements—Extends EAP (LEAP, PEAP, or EAP-transport layer security [TLS]) proxy to other RADIUS or external databases using standard RADIUS proxy
- Integration with Cisco's security management software applications—Provides a consolidated administrative TACACS+ control framework for many Cisco security management tools such as CiscoWorks VPN/Security Management Solution (VMS)

Competitive Products

- Funk: Steel Belted RADIUS
- Lucent/Avaya: Security Management Server(LSMS)
- Nortel: Preside RADIUS Server (OEM of Funk product)

Specifications

Feature	Cisco Secure Access Control Server (ACS) for Windows
Platform	Windows 2000 Server must meet the following minimum hardware requirements:Pentium processor, 550 MHz or faster; Minimum resolution of 256 colors at 800 x 600 lines
RAM	256 MB required; more if you are running your database onthe same machine
Disk Drive	250 MB of disk space; more if you are running yoru database onthe same machine
Software Requirements[1]	Cisco Secure ACS Server uses an English-language version of Windows 2000 Server. For specific types of service packs supported, refer to online documentation.The Windows server that runs Cisco Secure ACS must have a compatible browser installed. Cisco Secure ACS was tested with English-language versions of the following browsers on Microsoft Windows operating systems: Microsoft Internet Explorer 5.5 and 6.0, Netscape Communicator6.2
Platform Requirements	Cisco IOS Software 11.2 or higher on Cisco Routing Solutions

[1] Beginning with Cisco Secure ACS Version 3.1, Cisco Secure ACS on a Windows NT 4.0 server is no longer supported. For information about upgrading the operating system of a server running Cisco Secure ACS, see the Installation Guide for Cisco Secure ACS for Windows Server, Version 3.1

Selected Part Numbers and Ordering Information[1]

Cisco Secure Access Control Server (ACS) for Windows

CSACS-3.1-WIN-K9	Cisco Secure ACS 3.1 for Windows
CSACS-3.1-WINUP-K9	Upgrade to CSACS 3.1 for Windows from ACS versions 1.x, 2.x, 3.0 and Cisco Secure ACS for Unix version 2.x

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Secure ACS for Windows Web site: **http://www.cisco.com/go/acs**

Cisco Secure User Registration Tool

Cisco Secure URT is a virtual LAN (VLAN) assignment service that provides LAN security by actively identifying and authenticating users and then associating them only to the specific network services and resources they need through dynamic VLAN assignments to Cisco Catalyst® Switch networks. URT v2.5 introduces many innovative features, including a Web-based logon from Windows, Macintosh, and Linux clients, RADIUS and Lightweight Directory Access Protocol (LDAP) authentication, and a secure link between the client and the VLAN Policy Server (VPS). It also includes a security feature based on the Media Access Control (MAC) address that prevents users from accessing the network if they are not using authorized machines. Web based LAN authentication allows for user mobility within the LAN environment.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Secure User Registration Tool (URT)	• Web-based LAN authentication for Windows, Macintosh, and Linux client platforms—ideal for mobile users within the LAN environment • Extended security to protect user access to the logon VLAN from unregistered PCs through MAC-based security option • RADIUS authentication and accounting support • Multiple user access per port

Key Features

- Web Client Logon Interface—Supports customizable Web-based authentication for Windows, Macintosh, and Linux client platforms
- MAC-Based Security Option—Provides extended security to protect user access to the logon VLAN from unregistered PCs
- RADIUS Authentication and Accounting Support—RADIUS authentication is offered for Web logon
- Secure Link Between Cisco Secure URT Client and VPS Server—Security authentication and data encryption have been added to URT v2.5 to enable a more secure connection from the user
- LDAP Support (Active Directory and NDS directories)—Cisco Secure URT v2.5 supports Windows' Active Directory and Novell's NDS LDAP servers
- Multiple Users Per Port—Previous versions of Cisco Secure URT support only a single user logon on a single port
- Display of Windows NT Groups—The URT Administrator interface is enhanced to display the users belonging to a Windows NT group
- MAC Address Events History—With URT v2.5 MAC-address-based logon/logoff events are added as an option and reported to the history events tool

Specifications

Feature	Cisco Secure User Registration Tool (URT)
Server Requirements	Windows 2000 (SP2) server, professional, and Windows XP Professional-Min H/W (Pentium III, 512MB DRAM, 65 MB of disk space)
Browser for Web Login	Netscape version 4.79 and 6.2; IE version 5.5 (SP2) or 6.0
Client Software Requirements	Windows 98 (2ndE), Windows NT4 Workstation/Server (SP6A), Windows 2000 (SP2) Professional/server, Windows XP Professional, Windows XP Home (Web Client Only), Mac OS 10.1 (Web client only), Linux Redhat/ SuSE/ Mandrake/ VA (Web Client only)-Min H/W for Web client (Pentium II, 256MB DRAM, 65 MB of disk space), Min H/W for traditional client (Pentium II, 64MB DRAM, 1MB of disk space)
Supported Cisco Products (latest tested version)	1900 series (1912, 1924), v9.00.05; C2800 series (2822, 2828), v9.00.05; C2900XL series (2908XL, 2916XL, 2912XL, 2912LRE-XL, 2924XL, 2924LRE-XL), v12.0(5)WC3b; C2948GL3 series (2948GL3, 4232) v12.0(18)W5(22b); C2950 series, v12.1.6.EA2c; C3500XL series (3508XL, 3512XL, 3524XL, 3548XL, 3550XL), v12.0(5)WC3b; C3550 series, v12.1.8.EA1c; C4000 series (4003, 4006, 4912g), v7.1(2); C5000 series (2900, 2926, 2948, 5000, 5002, 5500, 5505, 5509), v6.3(5); C6000 series (6006, 6009, 6506, 6509, 6513), v7.1(3)

Selected Part Numbers and Ordering Information[1]

Cisco Secure User Registration Tool (URT)

URT-2.5-K9	Starter Kit: includes one (1) User Registration Tool 2.5 Software license, and one (1) Cisco 1101 VLAN Policy Server (VPS) appliance
URT-2.5-UP	Software only, upgrades customers from URT 2.X to 2.5; includes upgrade for both URT Admin Server and Cisco 1100 VPS appliance
URT-1101-HW-K9	Hardware Only; Cisco 1101 VPS appliance; additional appliance needed for backup, use in distributed deployments or deployments requiring Web logon capabilities

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco Secure User Registration Tool Web site: **http://www.cisco.com/go/urt**

CHAPTER 6

Content Networking Products

Content Networking Products at a Glance

Product	Features	Page
Cisco Content Engine 500 Series	Content services edge delivery platform for Enterprise networks • Functions as edge node device in an Application and Content Networking (ACN) system • Responsible for delivery of cachedor distributed content to the end-user • Enables customers to rapidly deliver strategic applications to branch personnel including web application andcontent acceleration,content filtering and business video • Lays the foundation foradvanced services such as e-learning and point of sale video delivery.	6-2
Cisco Content Engine 7300 Series	Content services platform for Enterprise data centerand Service Provider networks • Offers premium hosting services • Caching capabilities optimize Web site performance and WAN bandwidth utilization • Offers transparent and Internet proxy caching, Content Filtering and ECDN capabilities in a single platform • Accelerates both HTTP and streaming media file formats	6-2
Content Engine Network Modules	Content services edge delivery network module for 2600, 3600, 3700 branch routers • Functions as edge node device in an Application and Content Networking (ACN) system • Enables delivery of new applications and services via a Cisco branch router with no performance degradation of core routing services • Allows rapid delivery of strategic applications to branch personnelincluding web application and content acceleration,contentfiltering and business video	6-2
Cisco 11500 Series Content Services Switches	Next-generation intellgent platform for Web site and e-commerce optimization • Provides an intelligent, distributed architecture to scale for today's e-business infrastructure • Offers Adaptive Session Redundancy (ASR)—a new industry standard in stateful faibver • Delivers the greatest flexiblity of any content switch in its class for customizing combinations of ports, performance, andservices	6-4
Cisco LocalDirector	Integrated hardware and software solution for load balancing across servers • Allows many servers to appear as one server for high availability and easy scalability • Secure real-time embedded operating system	6-6
Cisco Content Distribution Manager 4600 Series	Content networking policy and management device • Central control over acquisition and distribution of content, including live and video on demand video, over IP networks • Intuitive web-based GUI provides integrated, easy-to-use managementover caching and content delivery functions such as multicast replication, intelligent cache bypass and bandwidth management • Roles based access control securely enables multiple administrators and content publishers across the organization	6-7
Cisco Content Router 4430	Integrated global loadbalancing solutionfor content delivery networks • Solves distributed server site selection problems • Uses HTTP (CR-4430) to redirect a client to the best site on the Internet based on network delay • Transparently redirection redirects end user requests to the end user and works with any IP application • Extremely fast site-selection algorithm is optimized for high performance Web-style transactions	6-9
Content Switching Module (CSM) for the Catalyst 6500 Series Switches	Line card for Catalyst 6500 • Balances client traffic across multiple servers within server farms • URL and Cookie-based load balancing • High-performance—200,000 new Layer 4 TCP connection setups per second	6-11
Cisco SSL Module for Catalyst 6500	• Offloads SSL encryption and decryption • Scalable performance • Stickyness	6-11

Product	Features	Page
Cisco 11000 Series Secure Content Accelerator (SCA 11000)	Appliance-based SSL solution • Offloads SSL encryption/decryption from Web servers • Supports 200 new SSL connections and 900 sustained SSL sessions per second • Interoperates withthe CSS 11000 for intelligent load balancingof SSL traffic	6-12
Cisco CTE-1400 Series Content Transformation Engine	Transforms Web and XML-based applicationsfor display and interaction on IPTelephones, PDAs, WAP Phones and other nonPC devices • Supports a broad range of end devices • Transforms existing applications • Design Studio GUI Application	6-13
Cisco DistributedDirector	Global Internet service scaling solution • Solves distributed server site selection problems. Enablesa set of distributed servers to be seen as a single virtual server • Uses DNS to redirect a client to the best site on the Internet basedon a variety of options • Configurable as authoritative Domain Name Services (DNS) cachingname server and/or HTTP Session Redirectoron a per-domain basis	6-14
Cisco GSS 4480 Global Site Selector	Global site selectionfor distributed datacenters • Delivers global load balancing for multipledata centers • Offloads Domain Named System (DNS) servers by doing DNS resolution • Scales to support hundreds ofdata centers orserver load balancers (SLBs)	6-15

Content Networking Overview

Cisco Content Networking solutions are designed to optimize the delivery of content to end users. To accomplish this, Cisco offers solutions for both data center and edge delivery with industry-leading products in both categories.

In the data center, Cisco Content Switching, or L4-7 Switching, solutions optimize any size network to dynamically enable faster responses to Web requests and decrease network bandwidth congestion. Content switching, or intelligent load balancing, insures high levels of content availability and security, and leverages investment in Cisco IP infrastructure.

Cisco's Application and Content Networking (ACN) System allows enterprises to accelerate mission critical web applications such as Siebel and SAP, block viruses and inappropriate web sites and deliver business video, while laying the foundation for advanced services such as e-learning and point of sale video delivery. For Service Providers, the Cisco ACN System represents a highly profitable, new revenue opportunity by enhancing the customer/user Web experience and significantly accelerating the delivery of rich Web applications, content and streaming media.

Cisco Content Engines

Within Cisco's content-networking solutions portfolio, the Cisco Application and Content Networking System (ACNS) Software enables a variety of services that optimize delivery of Web applications and content from the network edge to ensure enhanced speed, availability, and performance for users. ACNS Software combines the technologies of transparent caching and enterprise content-delivery network (ECDN) for accelerated delivery of Web objects, files, and streaming media from a single intelligent edge appliance, the Cisco Content Engine (CE).

The Cisco ECDN solution provides a platform that delivers immediate benefits from entry-level applications such as content and business application acceleration and URL filtering, while laying the foundation for advanced services such as business video and e-learning.

When to Sell

Sell This Product	When a Customer Needs These Features
Content Engine 7325	• Ultra high-end contentdelivery capabilities for advanced applications such as streaming media, e-learning, and corporate communications
Content Engine 7305	• High-end contentdelivery capabilitiesfor advanced applications such as streaming media, e-learning, and corporate communications
Content Engine 565	• Mid-range branch office and datacenter cache ideal for transparent caching, URL fitering, and edge content delivery
Content Engine 510	• Entry-level transparent caching and URL filtering capabilities along with limited contentdelivery
Content Engine Network Modules	• Router-integrated cachingand content delivery network modules for 2600, 3600, 3700 branch access routers

Key Features

- Caching—Provides accelerated content delivery, WAN bandwidth cost savings, and protection vs. uncontrollable bottlenecks
- Content Filtering—Enables administrators to block, monitor, and report on end users' access to non-business and objectionable content (uses N2H2 Internet Filtering Protocol, Secure Computing SmartFilter, or Websense Enterprise Software)
- Content Delivery—Use in conjunction with Cisco Content Distribution Manager to enable rich media e-learning and corporate communications; deliver new premium hosting services such as on-demand content delivery and streaming media; and, to scale Web sites

Competitive Products

- Blue Coat: Blue Coat ServerAccelerator 700 and 7000 Series and Blue Coat Systems Director
- Volera: Excelerator, Media Excelerator, Secure Excelerator
- Network Appliance: NetCache C1200/2100/6100 Series Appliances and Content Director

Specifications

Feature	Cisco Content Engine 7325	Cisco Content Engine 7305	Cisco Content Engine 565	Cisco Content Engine 510	Cisco CE Network Module	Cisco SA-7 and SA-14
Supported Interfaces	Two 10/100/1000BASE-TX	Two 10/100/1000BASE-TX	Two 10/100/1000BASE-TX	Two 10/100/1000BASE-TX	One internal 10/100-Mbps Ethernet to router backplane; one external 10/100-Mbps Ethernet	
SDRAM	4 GB	2 GB	1 GB	512 MB	Up to 512 MB	
Max Storage	936 GB	936 GB	396 GB	80 GB	396 GB	252 or 540 GB
	Ultra2 SCSI	Ultra2 SCSI	Ultra2 SCSI	IDE	Ultra2 SCSI	Ultra2 SCSI
Maximum Internal Storage	432 GB	432 GB	72 GB	80 GB	20 GB or 40 GB	252 or 540 GB
	Ultra2 SCSI	Ultra2 SCSI	Ultra2 SCSCO	IDE	IDE	Ultra2 SCSI
Flash Memory	128 MB	128 MB	128 MB	128 MB	16 MB internal; optional Compact Flash Memory	
Storage Array Support	Yes	Yes	Yes	No	Yes	
Rack Units	2 RU	2 RU	1 RU	1 RU	N/A	3 RU
Dimensions (HxWXD)	3.36 x 17.46 x 27.48 in	3.36 x 17.46 x 27.48 in.	1.72 x 17.3 x 16.75 in.	1.72 x 17.3 x 16.75 in.	One slot in 2600/3600/3700 chassis	5.0 x 17.5 x 20.4 in
Weight	62 lb.	62 lb.	28 lb.	28 lb.	1.5 lb.	76 lb.
Power	Hot-swappable redundant AC (DC availabled mid-2003)	Hot-swappable redundant AC (DC availabled mid-2003)	200W AC	200W AC	From 2600/3600/3700 chassis	AC (DC available mid-2003)

Selected Part Numbers and Ordering Information[1]

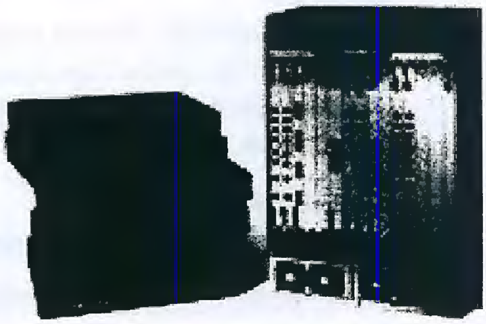
Cisco Content Engine 7300 Series Hardware	
CE-7325-K9	Content Engine 7325 AC Power, ACNSsoftware
CE-7305-K9	Content Engine7305 AC Power, ACNS software. Also runs as CDM or CR
Cisco Content Engine 500 Series Hardware	
CE-565-K9	Cisco Content Engine 565, AC Power, ACNS software. Also runs as CDM or CR
CE-510-K9	Cisco Content Engine 510 AC Power, ACNSsoftware
Cisco Content Engine Network Module Hardware	
NM-CE-BP-20G-K9=	Content EngineNetwork Module, basic performance,20-GB IDE hard disk
NM-CE-BP-40G-K9=	Content EngineNetwork Module, basic performance,40-GB IDE hard disk
NM-CE-BP-SCSI-K9(=	Content Engine Network Module, basic performance, SCSI controller (requiresexternal SCSI disk array such as the Cisco SA-6)

[1] This is only a small subset of all parts available via URL listed under "For More Information."

For More Information

See the Cisco Content Engine Web sites: **http://www.cisco.com/go/ce500** and **http://www.cisco.com/go/ce7300**

Cisco CSS 11500 Series Content Services Switches



The Cisco CSS 11500 Series Content Services Switch is suitable for both enterprises and service providers seeking to reduce data center costs, boost e-business application performance, offer enhanced services, ensure online transaction integrity, and provide the best possible online experience for customers, business partners, and internal workers.

The Cisco CSS 11500 is available in three models—the standalone Cisco CSS 11501, the three-slot Cisco CSS 11503 and the six-slot Cisco CSS 11506. Both the CSS 11503 and CSS 11506 systems take advantage of the same high-performance, modular architecture and use the same set of I/O, Secure Sockets Layer (SSL), and session accelerator modules. Also, all three systems operate with the same WebNS software, enabling the Cisco CSS 11501, 11503 and 11506 to offer industry-leading content switching functionality within three compact, hardware platforms.

When to Sell

Sell This Product	When a Customer Needs These Features
CSS 11501	• Standalone, fixed-configurationswitching platformwith up to 8 Fast Ethernet ports and 1 optional Gigabit Ethernet port • Cost-effective server, cache, and firewall load balancing • Complex Web applications requiring high-level URL and cookie switching
CSS 11503	• Compact, high-performance, modular content switching platform with up to 32 Fast Ethemet ports or up to six Gigabit Ethernet pots • Cost-effective server, cache, and firewall load balancing • Integrated SSL capabilities for secure transactions • Complex Web applications requiring high-level URL and cookie switching
CSS 11506	• Compact, high-performance, modular content switching platform with up to 32 Fast Ethemet ports or up to six Gigabit Ethernet pots • Cost-effective server, cache, and firewall load balancing • Integrated SSL capabilities for secure transactions • Complex Web applications requiring high-level URL and cookie switching

Key Features

- Introduces an intelligent, distributed architecture to meet the real-world scaling requirements of today's e-business infrastructure
- Improves site availability and transaction integrity by introducing Adaptive Session Redundancy (ASR)—a new industry standard in stateful failover
- Delivers the greatest flexibility of any content switch in its class for customizing combinations of ports, performance, and services
- Scales secured transaction performance through support of an integrated, high-capacity Secure Sockets Layer (SSL) module (WebNS 5.20)
- Protects investment by enabling upgrades of performance, ports, and services through modularity

Competitive Products

- Alteon/Nortel: ACEdirector and 700 Series
- F5 Networks: Big/IP and LAN switch Partners
- Foundry Networks: ServerIron
- Radware: Web Server Director (WSD)
- Resonate: Central Dispatch and GlobalDispatch

Specifications

Feature	Cisco CSS 11501	Cisco CSS 11503	Cisco CSS 11506
Modular Slots	N/A	3	6
Base Configuration	Switch Control with 8 10/100 Ethernet; 1 GBIC port	Switch Control Module 2 Gigabit Ethernet (GBIC) ports	Switch Control Module 2 Gigabit Ethernet (GBIC) ports
Max GB Ethernet Ports	1	6	12
Max 10/100 Ethernet ports	8	32	80
2-port GB Ethernet I/O Module		Max: 2	Max: 5
16-port GB Ethernet I/O Module		Max: 2	Max: 5
8-port GB Ethernet I/O Module		Max: 2	Max: 5
SSL Module		Max: 2	Max: 5
Session Accelerator modules		Max: 2	Max: 5
Redundancy features	Active-active Layer 5 Adaptive session redundancy Virtual IP Address (VIP) redundancy	Active-active Layer 5 Adaptive Session Redundancy VIP redundancy	Active-active Layer 5 Adaptive Session Redundancy VIP redundancy Active-standby SCM Redundant switch fabric module Redundant power supplies
Height	1/75 in. (1 rack unit)	3.5" (2 rack units)	8.75" (5 rack units)
Bandwidth	Aggregate 6 Gbps	Aggregate 20 Gbps	Aggregate 40 Gbps
Storage	512 MB hard disk or 256 MB Flash disk	512-MB hard disk or 256-MB Flash memory disk	512-MB hard disk or 256-MB Flash memory disk
Power	Integrated AC supply	Integrated AC or DC	Up to 3 AC or 3 DC

Selected Part Numbers and Ordering Information[1]

Cisco CSS 11500 Series Content Services Switches

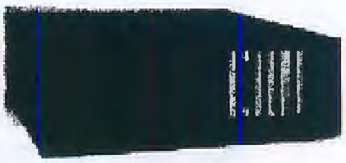
CSS11506-2AC	Cisco 11506 Content Services Switch including SCM with 2 Gigabit Ethernet ports,hard disk, 2 switch modules, 2 AC power supplies, and a fan (requires SFP GBICs)
CSS11506-2DC	Cisco 11506 Content Services Switch including SCM with 2 Gigabit Ethernet ports,hard disk, 2 switch modules, 2 DC power supplies, and a fan (requires SFP GBICs)
CSS11503-AC	Cisco 11503 Content Services Switch including SCM with 2 Gigabit Ethernet ports, hard disk, and integrated AC powersupply, integrated fan,and integrated switch module (requires SFP GBICs)
CSS11503-DC	Cisco 11503 Content Services Switch including SCM with 2 Gigabit Ethernet ports, hard disk, and integrated DC powersupply, integrated fan,and integrated switch module (requires SFP GBICs)
CSS5-SCM-2GE	Cisco CSS 11500 System Control Module with 2 Gigabit Ethemet ports and hard disk (requires SFP GBICs)
CSS5-IOM-8FE	Cisco CSS 11500 Fast Ethernet I/O Module:8-port TX
CSS5-IOM-16FE	Cisco CSS 11500 Fast Ethernet I/O Module:16-port TX
CSS5-IOM-2GE	Cisco CSS 11500 Gigabit Ethernet I/O Module: 2-port (requires SFP GBICs)
CSS5-SAM	Cisco CSS 11500 Session Accelerator Module
CSS5-SSL	Cisco CSS 11500 SSL Module
CSS11501	Cisco CSS 11501 Content Services Switch-8 Fast Ethemet, hard disk, AC

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the CSS 11500 series Web site: **http://www.cisco.com/go/11500**

Cisco LocalDirector



The Cisco Local Director Series offers a high-availability, integrated hardware and software solution that intelligently balances the load of user traffic across multiple TCP/IP application servers. Cisco Local Director tracks network sessions and server load conditions in real time, directing each session to the most appropriate server. All physical servers appear as one virtual server, requiring only a single IP address and a single URL for an entire server farm.

A key component of a content delivery network, Cisco Local Director accelerates content delivery by routing client requests to the best Web server at the Web site of origin. Cisco Local Director supports critical content routing protocols such as Dynamic Feedback Protocol (DFP) and the Boomerang Control Protocol (BCP), which ensure seamless content delivery network integration and reduced deployment costs. Layer 4-7 content load balancing guarantees that the correct client is routed to an optimized content location. The accelerated server load balancing (ASLB) feature works with the Cisco Catalyst 6000 and 6500 Series switches to accelerate scaling of TCP sessions and help to protect against Flash crowds—sudden traffic surges that can overwhelm a web site.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco LocalDirector	• Load balancing acros multiple TCP/IP application severs • High availability Internet services such as e-commerce, Web content, ande-mail • High availability Intranet services for employees, customers, and suppliers

Key Features

- HTTP redirect sticky enables client-to-server persistence, regardless of SSL and shopping-cart configurations, to improve site availability
- Hot-standby and stateful failover mechanisms ensures high availability by eliminating all points of failure for the data center
- Transparent support for all common TCP/IP Internet services, including User Datagram Protocol (UDP), accommodates a wide range of applications and communications needs (Web, File Transfer Protocol [FTP], Telnet, Domain Name System [DNS], and Simple Mail Transfer Protocol [SMTP]) without special software configuration
- SSL and cookie sticky ensures completion of complex transactions in proxy server environments
- Client-assigned load balancing provides QoS mechanism by allowing traffic to be directed to servers based on source IP address
- High-performance hardware supports six Fast Ethernet (Cisco Local Director 417) or two Fast Ethernet plus two Gigabit Ethernet (Cisco Local Director 417G) interfaces
- Network Address Translation (NAT) allows unregistered IP addresses on servers without router assistance

- Simple setup in 10 commands offers simple setup for typical configurations, with little disruption to existing network configuration and no changes to network addresses
- Integrated security capability effectively protects server farms from unauthorized access by filtering based on client IP address and service

Competitive Products

- F5 Labs: Big IP
- Foundry Networks: ServerIron Switch
- Nortel Networks/Alteon: Ace Director
- Radware: Web Server Director
- Resonate, Inc.:Central Dispatch

Specifications

Feature	LocalDirector 417	LocalDirector 417G
Supported Interfaces	Six 10/100 BASE-TX	Two 10/100BASE-TX plustwo 1000BASE-SX interfaces
Other Interfaces	RJ-45 console interface; DB-15 redundant failover interface	RJ-45 console interface; DB-15 redundant failover interface
RAM	512 MB	512 MB
Flash	16 MB	16 MB
Performance	8000 virtual and real IP addresses 700,000 simultaneous TCP connections 80-Mbps throughput	64,000 virtual and real IP addresses 1,000,000 simultaneous TCP connections 400-Mbps throughput400
Dimensions (HxWXD)	1.72 x 17.5 x 14.13 in	1.72 x 17.5 x 14.13 in

Selected Part Numbers and Ordering Information[1]

Cisco LocalDirector

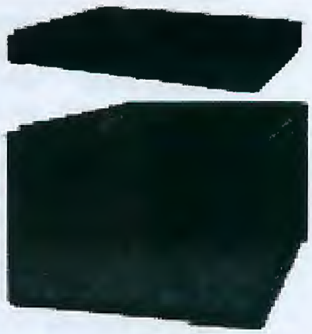
LDIR-417	Cisco Local Director 417
LDIR-417G	Cisco Local Director 417G

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the LocalDirector Web site: **http://www.cisco.com/go/ld**

Cisco Content Distribution Manager 4600 Series



The Cisco Content Distribution Manager (CDM) configures network and device policy settings for edge node Content Engines (CE). Used to accelerate web content and save network bandwidth in a content networking architecture, the CDM can be easily integrated into existing network infrastructures. Deployed in an Enterprise or Service Provider Internet or extranet environment, the Cisco CDM and CEs provide transparent on-demand rich media streaming and static file delivery to standard PCs.

Cisco Enterprise Content Delivery Networks (ECDNs) allow service providers and enterprises to distribute rich media content closer to their target customers overcoming issues such as network bandwidth availability, distance or latency obstacles, origin server scalability, and congestion issues during peak usage periods. The ECDN solution enables content delivery services for web hosting, streaming, e-commerce, e-learning, corporate communications, and mission critical e-business applications.

When to Sell

Sell This Product	When a Customer Needs These Features
CDM 4630	• Low-cost early deployment, or small enterprise network trials, proof of concept, and pilot programs
CDM 4650	• Medium and large enterprise networks, supports up to 1000 Cisco Content Engines
CDM 4670	• Service provider deployment, supports thousands of Cisco Content Engines

Key Features

- Complete CDN solution with Cisco Content Router and Cisco Content Engines
- Central control over delivery of high-bandwidth content, live and video-on-demand over any IP network
- Easy-to-use management capabilities through a Web-based GUI; services include previewing and scheduling replication of media to edge devices, bandwidth and content management
- Automatically generates thumbnail reference images and sample Web pages for integration with corporate extranet, intranet, and Internet sites
- One URL per media file provides seamless integration into any Web site
- Integrates with standards for Web multimedia presentation, including HTML/DHTML, eXtensible Markup Language (XML) and SMIL
- Secure and fault-tolerant file transfer using Secure Socket Layer (SSL) encryption for secure media transfers
- Channel configuration for media distribution to any number of discrete audiences using "distribution lists"
- Host content for a variety of customers within a single CDN
- Ability to create multiple virtual CDNs addressing targeted media distribution
- Content registration in cache logs for billing capabilities

Competitive Products

- Cacheflow: Client and Server Accelerators
- Inktomi: Traffic Server
- Network Appliance: ContentDirector

Specifications

Feature	Content Distribution Manager 4630	Content Distribution Manager 4650	Content Distribution Manager 4670
Sampling of Rich Media File Formats	MPEG RealVideo Windows Media QuickTime HTML, GIF, JPEG Adobe Acrobat Macromedia Shockwave CAD/CAM MRI	Same as CDM 4630	N/A—file formats handled by the CEs
Supported Interfaces	Autosensing 10/100BASE-T	Autosensing 10/100BASE-T	Autosensing 10/100BASE-T
Recommended Network Size	Less than 100 CEs	Less than 1000 CEs	Less than 10,000 CEs
Processor Speed	600-MHz PIII	2x866 Xeon	2x866 Xeon
RAM	512 MB	1 GB	1 GB
Internal Storage	One 30 GB, 10K RPM, Ultra2 SCSI disk drive	140 GB RAID 5	36 GB[1]
Rack Units	1	7	7
Dimensions (HxWXD)	1.72 x 17.5 x 14.1 in.	12.25 x 17.5 x 28 in.	12.25 x 17.5 x 28 in.

[1] Minimum storage required for DM service provider configurations

Selected Part Number and Ordering Information[1]

Cisco Content Distribution Manager 4600 Series Hardware	
CDM-4630	Cisco Content Distribution Manager 4630
CDM-4650	Cisco Content Distribution Manager 4650
CDM-4670	Cisco Content Distribution Manager 4670

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Content Distribution and Management Web site:
http://www.cisco.com/go/cdm

Cisco Content Router 4430

The Cisco Content Router 4430 (CR 4430) is a compact, high-performance solution for enabling premium Web services over public or private networks. Featuring either Cisco Enterprise Content-Delivery Network (ECDN) or Content Router 1.1 Software, customers can transparently route user Web browsers to the optimal content engine for file delivery.

With its patented routing technology, the Cisco CR 4430 provides redundancy, scalability, and performance enhancements for network Web sites in either an enterprise or public service provider network. Using Hypertext Transfer Protocol (HTTP)-based re-direction, the Cisco CR 4430 can redirect users over the public network or behind the security of a corporate firewall, making it a vital component of the Cisco end-to-end Content Networking Solution.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Content Router 4430	• When a customer needs to support a Cisco Enterprise Content Delivery Network with HTTP redirection • Supports resiliency for ECDNs when used with a Cisco CSS 11500 content services switch • Up to five Cisco CR 4430s can be deployed in an ECDN network to provide greater network availability and performance

Key Features

- Uses HTTP to redirect a client to the best site on the Internet based on network delay
- Transparent redirection to the end user and works with any IP application
- Easy configuration through a Cisco IOS-style command-line interface
- Redundant configurations, multiple CRs can be deployed at the origin site to provide fail-over and load scaling

Specifications

Feature	Cisco Content Router CR4430
Network Interface Card	10/100BASE-TX
Processor	600- MHz PIII
RAM	1 GB
Internal Storage	18 GB
Rack Units	1
Dimensions (HxWXD)	1.72 x 17.50 x 14.13 in.
Weight	12.5 lbs.

Selected Part Number and Ordering Information

Cisco Content Routers

CR-4430	Contentrouter that utilizes HTTP redirection for usewith the ECDN product

For More Information

See the Cisco Content Router Web site: **http://www.cisco.com/go/cr**

Cisco Content Switching Module

The Cisco Content Switching Module (CSM) is a Catalyst 6500 line card that balances client traffic to farms of servers, firewalls, SSL devices, or VPN termination devices. The CSM provides a high-performance, cost-effective load balancing solution for enterprise and Internet Service Provider (ISP) networks. The CSM meets the demands of high-speed Content Delivery Networks, tracking network sessions and server load conditions in real time and directing each session to the most appropriate server. Fault tolerant CSM configurations maintain full state information and provide true hitless failover required for mission-critical functions.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Content Switching Module	• An integrated bad balancing solution featuring Cisco's Catalyst 6500 • Load balancing for the highes traffic sights • Support for up to 1,000,000 concurrent TCP connections

Key Features

- Market-leading performance—Establishes up to 200,000 Layer 4 connections per second and provides high-speed content switching, while maintaining 1 million concurrent connections
- Outstanding price/performance value for large data centers and ISPs—Features a low connection cost and occupies a small footprint. The CSM slides into a slot in a new or existing Catalyst 6500 and enables all ports in the Catalyst 6500 for layer 4 through layer 7 content switching. Multiple CSMs can be installed in the same Catalyst 6500
- Uses the same Cisco IOS Command Line Interface (CLI) that is used to configure the Catalyst 6500 Switch

Competitive Products

- Alteon/Nortel: ACEdirector and 700 Series
- Radware: Web Server Director (WSD)
- F5 Networks: Big/IP and LAN switch Partners
- Foundry Networks: ServerIron
- Resonate: Central Dispatch and GlobalDispatch

Specifications

Feature	Cisco Content Switching Module (CSM)
Configuration Limits	256 total VLANs (client and server); 4000 virtual servers; 4000 server farms; 16,000 real servers; 4000 probes; 16,000 access control list (ACL0 items
Connections	1,000,000 concurrent TCP connections 200,000 connection setups per second-Layer 4
Throughput	4 Gigabits-per-second total combined (client-to-server and server-to-client) throughput
Catalyst Switch Platform Requirements	Cisco IOS Software only—Catalyst Operating System is not supported Functions as a bus enabled line card—not fabic enabled Multilayer switch feature card-MSFC or MSFC2

Selected Part Numbers and Ordering Information[1]

Cisco Content Switching Module	
WS-X6066-SLB-APC	Catalyst 6500 Content Switching Module

For More Information

See the Catalyst 6500 Series Web site at: **http://www.cisco.com/go/cat6500**

Cisco SSL Module for Catalyst 6500

The SSL Services Module is an integrated service module for the Cisco Catalyst® 6500 Series that offloads the processor-intensive tasks related to securing traffic with Secure Sockets Layer (SSL) and increases the number of secure connections supported by a Web site.

When to Sell

Sell This Product	When a Customer Needs These Features
SSL Module for Catalyst 6500	• An integrated SSL encryption/decryption solutionfeaturing Cisco's Catalyst 6500 • Scalable SSL processing: 2,500 connectionsetups/second permodule-10,000 per Chassis fully-populated with SSL modules

Key Features

- Server SSL offload—performs all SSL-related tasks, allowing servers to handle high-speed clear text traffic
- Scalable performance—provides a simple means of addressing increased performance requirements by installing additional SSL modules in a Catalyst 6500 switch
- Stickyness—maintains persistence even when clients request new session IDs, in Integrated Mode with Content Switching Module (CSM)
- Certificate optimization—provides cost savings by requiring only a single certificate copy vs. a copy for each server subject to customer and certificate authority agreement

Competitive Products

• F5 Networks eCommerce 540	• Nortel/Alteon iSD 410 SSL Accelerator

Specifications

Feature	Cisco SSL Module for Catalyst 6500
System Capacity and Performance	2500 connection setups/sec per module-10K per chassis; 60K concurrent client connections-240K per chassis; 300 Mbps bulk rate encryption-1.2 Gbps per chassis; 256 key pairs; 256 key certificates; Up to 2K key sizes,256 proxy servers
Scalability	Up to four SSL modules in the same Catalyst 6500
Integration with Server Load Balancing	Tightly integrated in the Cisco Catalyst 6500 Switch with the CSM

Selected Part Numbers and Ordering Information[1]

Cisco SSL Module for Catalyst 6500	
WS-SVC-SSL-1-K9=	Cisco SSL Module for Catalyst 6500

For More Information

See the Catalyst 6500 Series Web site at: **http://www.cisco.com/go/cat6500**

Cisco 11000 Series Secure Content Accelerator (SCA 11000)

The Cisco 11000 Series Secure Content Accelerator (SCA 11000) is an appliance-based solution that increases the number of secure connections supported by a Web site by offloading the processor-intensive tasks related to securing traffic with SSL. Available in two versions, the SCA 11000 simplifies security management and allows Web servers to process more requests for content and handle more e-transactions.

Key Features

- Offloads all encryption, decryption, and secure process for a Web site, freeing Web servers to perform essential Web tasks and eliminating the need for SSL server software
- Boosts e-commerce site performance up to 50 times through dedicated SSL processing hardware—supports 200 or 800 new SSL connections per second
- Centralizes and manages the widest range of digital certificates to ensure complete independence from the Web server
- Provides linear scalability and fault tolerance—interoperates with the Cisco 11500 series Content Services Switches (CSS 11500) for intelligent load balancing of SSL traffic
- Works with any Web server platform to provide SSL support for any Web site
- Installs quickly and easily with very low maintenance—no special software required on Web servers or Cisco 11500 series switches

Specifications

Cisco SCA 11000	SCA2	SCA
Number of Ports	Two 10/100BaseTX Ports	Two 10/100Base TX Ports
Port Description	Network Ports: Two 10/100Base TX; Console Port: DB9 Serial Port; Failover Port: DB9 Serial Port	Network Ports: Two 10/100Base TX; Console Port: DB9 Serial Port; Failover Port: DB9 Serial Port
Data Transfer Rates	Ethernet: 10 Mbps (half duplex), 20 Mbps (full duplex)Fast Ethernet: 100 Mbps (half duplex), 200 Mbps (full duplex)	Ethernet: 10Mbps (half duplex), 20 Mbps (full duplex) Fast Ethemet: 100 Mbps (half duplex), 200 Mbps (full duplex)
Configuration Software OS Support	Windows NT 4.0; Red Hat Linux 5.0, 6.0, 6.1, 6.2	Windows NT 4.0; Red Hat Linux 5.0, 6.0, 6.1, 6.2
Memory	64 MB RAM; 16 MB Flash ROM	64 MB RAM; 16 MB Flash ROM
Dimensions	8.875 x 1.75 x 19 in.	8.875 x 1.75 x 19 in.
Connection Rates	800	200
Concurrent Sessions	5,000	30,000

Selected Part Numbers and Ordering Information

Cisco SCA 11000	
CSS-SCA-2FE-K9	CSS Secure Content Accelerator
CSS-SCA2-2FE-K9	CSS Secure Content Accelerator version 2

For More Information

See the Cisco SCA 11000 Web site: **http://www.cisco.com/go/sca11000**

Cisco CTE-1400 Series Content Transformation Engine

The Cisco CTE 1400 Series Content Transformation Engine provides customers with a high-performance, appliance-based solution that delivers real business applications and Internet content to a variety of devices including Wireless Application Protocol (WAP) phones, personal digital assistants (PDAs), Blackberry pagers, Cisco IP Phones and other non PC devices. Examples of applications that can be transformed include e-mail, CRM/SFA applications, intranets, maps, directions, and corporate directories as well as many vertical applications in healthcare, retail, finance, hospitality and education. The Content Transformation Engine (CTE) is a 1 Rack Unit appliance optimized to perform the task of converting HTML and XML applications to a format appropriate for devices with unique display requirements. In addition, the solution recognizes specific Web-enabled devices such as IP Phones, PDAs and mobile phones, and customizes the delivery of information to give users the right form of data, to suit their devices characteristics, capability as well as the usage model.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco CTE-1400 Series Content Transformation Engine	• Quickly and easily transform applicationsto extend them to a variety of new devices. • Low total cost of ownership (TCO) • Immediate results for a rapid return on investment • Self-contained applianceoptimized for transformation

Key Features

- Self-contained appliance for content transformation; includes DesignStudio for defining transformation rules
- Seamlessly transforms content as it moves from server to the target device, leaving the server and underlying data unchanged; Reformats data into all major Markup Languages
- Supports Cisco's AVVID architecture, including transformation for Cisco IP telephony
- Low total cost of ownership

Specifications

Feature	Cisco CTE-1400 Series Content Transformation Engine
Rack Units	1
Dimensions (HxWxD)	1.70 x 16.7 x 22in.
Weight	23 lbs

Selected Part Numbers and Ordering Information[1]

Cisco CTE 1400 Series Content Transformation Engine

CTE-1450-K9	Content Transformation Engine Hardware
CTE-WAP=	WAP module for CTE 1400 Series
CTE-PALM=	Palm module for CTE 1400 Series
CTE-RIM=	RIM Blackberry module for CTE 1400 Series
CTE-HTML=	HTML module for CTE 1400 Series

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the CTE-1400 Series Web site at **http://www.cisco.com/go/cte**

Cisco DistributedDirector[1]

DistributedDirector provides dynamic, transparent, and scalable Internet traffic load distribution between multiple geographically-dispersed servers. DistributedDirector is a global Internet service-scaling solution that utilizes Cisco IOS software and leverages routing table information, delay characteristics, and other information to make "network intelligent" load distribution and site selection decisions.

DistributedDirector transparently redirects end-user service requests to the closest responsive server, which increases access performance and reduces transmission costs. Users need only a single subdomain name or URL-embedded hostname for accessing a distributed set of servers, thus providing the appearance of a single virtual server.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Distributed Director	• Load distribution across geographically/topologically dispersed TCP/IP servers • High availability for dispersed mission-critical applications • Data center redundancy and failover

Key Features

- Transparent distribution of all IP Services (TCP and UDP), including HTTP, FTP, Telnet, and Gopher; provides global scalability for all IP-based network services
- Improves access performance by redirecting to the topologically closest server
- Calculates client-to-server round-trip times in real time; redirects clients to server with lowest client-to-server link latency, maximizing end-to-end performance
- Redirects clients only to responsive servers, resulting in maximized availability
- Cisco IOS Software & standard command line interface for device configuration
- Transparently add and remove distributed servers, simplifying maintenance
- Supports multiple domains; cost-effective IP service scalability solution

Competitive Products

- Alteon Networks: ACEdirector and Web Switches with WebOS GLSB
- F5 Labs: 3DNS
- Foundry Networks: ServerIron Switch with Internet IronWare
- Resonate, Inc.:Global Dispatch
- RND Networks, Inc.: Web Server Director - Network Proximity (WSD-NP)

For More Information

See the DistributedDirector Web site at **http://www.cisco.com/go/dd**

[1] **DistributedDirector is available in Cisco IOS software for 2600/2600XM, 3600, and 7200 series routers, starting on release 12.2(4)T Enterprise Plus feature sets; Dedicated routers may be recommended for DistributedDirector to meet performance targets of both routing and load balancing; If no dedicated hardware platform is available for running DistributedDirector, it is recommended customers use the Configurable DD Cache feature (available in 12.2(8)T) to limit the memory DistributedDirector may consume for DNS caching; To take advantage of enhanced caching capabilities, routers should be configured with additional DRAM (128MB or more)**

Cisco GSS 4480 Global Site Selector

The Cisco GSS 4480 is a networking product that globally load balances distributed data centers. The Cisco GSS 4480 acts as the cornerstone of multisite disaster recovery plans in deployments of Cisco's market-leading content switches. Customers deploying new Cisco content switches such as the Cisco CSS 11500 Content Services Switch and the Content Switching Module (CSM) for the Cisco Catalyst ® 6500 Series switches or have already deployed legacy switches such as the Cisco CSS 11000 and Cisco Local Directors can benefit from the new levels of traffic management and centralized command and control provided by the Cisco GSS 4480.

Key Features

- Provides resilient architecture critical for disaster recovery and multisite Web applications deployments
- Offers flexible heterogeneous support for all Cisco SLBs and DNS-capable networking products
- Provides centralized command and control of DNS resolution process for direct and precise control of global load-balancing process
- Offers site persistence for e-commerce applications
- Offers a unique DNS race feature-The Cisco GSS 4480 can in real time direct content consumers to the closest data center
- Supports a Web-based graphical user interface (GUI) and DNS wizard to simplify the DNS command and control

Competitive Products

- F5 Networks eCommerce 540
- Nortel/Alteon iSD 410 SSL Accelerator

Specifications

Feature	Cisco GSS 4480
Number of Ports	Two 10/100Base TX Ports
Port Description	Network Ports: Two 10/100Base TX; Console Port
DNS requests per second	4000, dependingon configuration(~ 345 million DNS requests per day per Cisco GSS 4480; an entire system is capable of 2.7 billion DNSrequests per day)
Configuration Software OS Support	Windows NT 4.0; Red Hat Linux 5.0, 6.0, 6.1, 6.2
Network management	Console port-CLI Access to system via Telnet; Secure copy(SCP) or FTP; GUI-Secure HTTP (HTTPS) for Internet Exploer and Netscape Navigator
Storage	One 36-GB hard drive
Physical	One-rack unit size chassis; Network management serial port1 GB of RAM600-MHz PIII CPU
Dimensions	1.72 x 17.5 x 14.13 in. (43.7 x 444.5 x 358.9 cm)

Selected Part Numbers and Ordering Information[1]

Cisco GSS 4480

Cisco GSS 4480-K9	Global site selector
SF-GSS-V1.0-K9	SF-GSS-V1.0-K9Global site selector software

For More Information

See the Cisco GSS 4480 Web site: **http://www.cisco.com/go/gss**

CHAPTER 7

Broadband and Dial Access Products

Broadband and Dial Access Products at a Glance

Remote Dial Access—Data and Voice (VoIP)

Product[1]	Features	Page
Cisco AS5350 Series Universal Gateways	• High performance,1RU, universal gateway • Universal Port technology formultiple data, voice, and faxservices on anyport at any time • 2,4, & 8 CT1/7 CE1/PRI configurationsfor 48 to 240 channels • Supports broad range of async/ISDN/VoIP/wireless protocols • Two 10/100 Ethernet ports,two 8 Mbps serial backhaul ports • Two 8 Mbps serial backhaul ports • Cisco SS7 signaling gatewayinteroperability • Flexible, redundant backhaulmethods	7-3
Cisco AS5400 Series Universal Gateways	• High performance,2RU, universal gateway • Universal Port technology formultiple data, voice, and faxservices on anyport at any time • Two models: Cisco AS5400HPX and Cisco AS5400 • 8 to 16 CT1/CE1/PRI or 1 T3 configuration for 192 to 648 channels • Low power and high availability design • Supports a broad range of async/ISDN/VoIP/fax/wireless protocols • Cisco SS7 signaling gatewayinteroperability • Flexible, redundant backhaulmethods	7-6
Cisco AS5850 Universal Gateway	The highest density universal gatewayin the marketplace • Supportingup to 5 x CT3s, 96 T1s or 86 E1s of multiple data, voice, and fax services on any port at any time • Constant density regardless of codectype, ECAN or VAD settings • Extensive high availability features • TDM grooming capability	7-9
Remote Dial Access Network Management	Suite of network management products for configuration, troubleshooting,and maintenance of Cisco dial access and VoIP solutions	7-11
SS7 Signaling & Softswitch Products	• Cisco PGW 2200 Softswitch—Call Agent providing signaling and call controlfunctionality for PSTN Gateway and transit applicationsin international markets • Cisco BTS 10200 Softswitch—MGCP-basedsoftswitch for large-scale Voice over IP and ATM applications	7-12

[1] For Cisco 2509 and 2511 Access Servers, see page 1-14.

Broadband Cable

Product	Features	Page
Headend and Distribution Hub Equipment		
Cisco uBR7100 Series Universal Broadband Router	Entry-level, fixed-configuration CMTS and integrated outer for lower-density residential and MxU customers serviced by Tier 2/Tier 3 cable operators or ISPs. • Choice of four DOCSIS- and EuroDOCSIS-qualified, fixed-configuration modelsthat include: Cisco uBR7111, Cisco uBR7111E, Cisco uBR7114, and Cisco uBR7114E • Integrated upconverter/modulatoron the cable interface • Embedded dual 10/100 BaseT Ethernet network interface • Additional network interface with a variety of LAN and WAN options • Supports up to 1,000[1] data customers	7-13
Cisco uBR7246VXR Universal Broadband Router	• Modular, standards-based communications-grade CMTS and integrated router for high-growth broadband cable deploymentsSupports up to 8,000 subscribers and offers a large variety of LAN and WAN interface options and processors	7-15

Product	Features	Page
Cisco uBR10012 Universal Broadband Router	Highest-capacity communications-grade CMTS and integrated router on the market today that delivers the services, perfomance, scale, and carrier-class reliability large cable operators and ISPs demand • High-performance aggregationplatform that uses Parallel Express Forwarding technology • Eight cable line cards that include support for Cisco Universal Broadband Router (uBR) line cards and the Cisco 5X20 Broadband Processing Engine (BPE) • Four network interfaces that include support for 1 Gbps over Gigabit Ethernet, 622 Mbps over OC-12 Packet over SONET, and OC-48-Dynamic Packet Transport (DPT) Interface Module Set • Cisco uBR10012 supports up to 80,000[1] subscribers	7-16
Cisco RF Switch	• Exceeds PacketCable Availability Requirements • Enables a fully redundant CMTS withno single point of failure;works with the Cisco uBR7246VXR and uBR10012 • Maximizes density with more than 250 MCX-type connector	7-17
Customer Premise Equipment (CPE)		
Cisco uBR900 Series Cable Access Router	Integrated DOCSIS-based cable modem and router with hardware accelerated IPSec VPN tunneling support that includes: • Cisco uBR925 with 4 Ethernet, 1 CATV, 1 USB and 2 FXS ports that support telecommuter and small office DOCSIS-based data, VoIP, and VPN services • Cisco uBR905 with 4 Ethernet and 1 CATV port that supports DOCSIS-based data and VPN services	7-19

1. Numbers are for reference only. Actual numbers for specific systems will vary depending on network/service loading, traffic, and other parameters.

DSL (Digital Subscriber Line) Access

Product	Features	Page
DSL Access CPE[1]	Wide variety of Cisco router-based DSL CPE solutions for business-class to small office applications	7-21
Broadband Services Aggregation	• Cisco 6400 Series Router—ATM switching core, with up to 48,000 subscriber sessions per chassis • Cisco 7200 Series Router—Up to 16000 broadband sessions on a 3 RU platform, including aggregation of PPP, PPPoE, and PPPoA • Cisco 7301 Series Router—1 RU Broadband Aggregation Router that is capable of delivering up to 16000 sessions per chassis • Cisco 7400 Series Router—1 RU broadband optimized applance that delivers up to 8,000 sessions per chassis • Cisco 10000 Series Router—A carrier-class router that supportsup to 32,000 broadband sessions with 99.999 percent system uptime	7-21

1. For ADSL, ISDN, and IDSL small office/home office (SOHO) customer premise equipment (CPE), see Chapter 1: Routers

ATM Multiservice WAN Switching

Product	Features	Page
Cisco BPX 8600 Series Switches	• Large-scale AdvancedATM switch for service provider and large enterprise applications • Narrowband and broadband services in a single, highly reliable platform using a multishelf architecture with intelligent call processing for Frame Relay and ATM switched virtual circuits (SVCs) • 20 Gbps of high-throughput switching for multiple traffic types data, voice, and video	7-23
Cisco MGX 8850 Series Advanced ATM Multiservice Switches	• Multiservice switch, scales from DS0 to OC-48c/STM-16 speeds • Serves as a stand-alone device for narrowband services, an integrated edge concentrator or a broadband edge switch when equipped with 45 Gbps switch card and broadband ATM modules	7-24
Cisco MGX 8830 Series Multiservice Switches	• Multiservice switch scales from from DS0 to OC-3c/STM-1 speeds • A standalone switch with narrowband interfaces and broadband trunking to remote sites with low density and high service mix requirements with 1.2 Gbps switch fabric	7-25
Cisco IGX 8400 Series Multiservice WAN Switches	• ATM-based WAN switching, connects to public services for reduced leased-line costs • Available with 8, 16, or 32 slots	7-25
Cisco MGX 8200 Series Multiservice Gateways	• Edge concentratorsfamily provide a cost-effective narrowband multiservice solution for low to mid-band ATM and Frame Relay aggregation with QoS management features	7-25

Long Reach Ethernet

Product	Features	Page
Cisco Catalyst 2950 LRE XL Switches	Fixed configurationEthernetswitchesfor delivering converged voice, video, and data services over existing category 1/2/3 wiring for the MxU and enterpise markets. • 12- or 24-port 1RU switchesystems with four 10/100 ports, deliver Ethernet traffic (up to15 Mbps) over standard copper cabling (up to 5000 feet); idealfor MxU broadband Internet access • Co-exists with POTS and ISDN traffic on the same line and compatible with ADSL • Advanced qualityof service for supporting converged voice, video, and data services	7-26
Cisco LRE CPE Devices	• Cisco 575 LRE CPE—Compact, includes one RJ-45 Ethernet connection and two RJ-11 connectors(for telephone) • Cisco 585 LRE CPE—Compact, includesfour RJ-45 switched Ethernet connectios and two RJ-11 connectors (for telephone).Supports 802.1p QoS	7-27
Cisco LRE POTS Splitter	• Cisco LRE 48 POTS Splitter—48 ports in 1RU. Ensures that POTS service is separate, and never compromised by LRE switch reconfiguration or downtime	7-27
Cisco Broadband Building Service Maneger	• Server system enables automated onlne activation, integratedbilling, tiered service levels • Ideal for any form of broadband accesstechnology, including Ethernet, LRE, Cable access, DSL, Wireless, or Fiber	7-28

Memory Information for Access Routers

Router	Memory Type	Slots	Default Memory	Max Memory	Default Config. (Notes)
Cisco AS5350 Universal Gateway	System Flash SDRAM Shared Boot Flash	N/A	32 MB 128 MB 64 MB 8 MB	64 MB 512 MB 128 MB 16 MB	
Cisco AS5400HPX Universal Gateway	Main SDRAM Shared Boot Flash (3V) System Flash (3V)	2 1 1 2	256 MB 64 MB 8 MB 32 MB	512 MB 128 MB 16 MB 64 MB	Cisco AS5400HPX and Cisco AS5400 use different Boot and System Flash — NOT interchangeable
Cisco AS5400 Universal Gateway	Main SDRAM Shared Boot Flash (5V) System Flash (5V)	2 1 1 2	256 MB 64 MB 8 MB 32 MB	512 MB 128 MB 16 MB 64 MB	Cisco AS5400HPX and Cisco AS5400 use different Boot and System Flash — NOT interchangeable
Cisco AS5850 Universal Gateway	RSC SDRAM Feature Cards SDRAMS		512 MB 128 MB	512 MB 128 MB	Ships with all required memory
Cisco CVA120 Series	Config NVRAM DRAM Flash		128 kB 16 MB 8 MB		

Cisco AS5350 Universal Gateway

The Cisco AS5350 Universal Gateway is the only one-rack-unit gateway supporting two-, four-, or eight-port T1/seven-port E1 configurations that provides universal port data, voice, and fax services on any port at any time. The Cisco AS5350 Universal Gateway offers high performance and high reliability in a compact, modular design. This cost-effective platform is ideally suited for Internet service providers (ISPs) and enterprise companies that require innovative universal services.

The Cisco AS5350 Universal Gateway eliminates the need for switches and routers to create a point-of-presence (POP) or "POP-in-a-box" solution. The Cisco AS5350 Universal Gateway has three primary universal gateway configurations: two Channelized T1(CT1)/Channelized E1(CE1)s, four CT1/CE1s, and eight CT1/seven CE1s . It also includes integrated signaling link termination (SLT) functionality for direct connection to a SS7/C7 signaling gateway.

The Cisco AS5350 Universal Gateway comes two high-speed serial ports are provided to support Frame Relay, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC) backhaul. All backhaul interfaces support Hot Standby Router Protocol (HSRP), and all cards and the fan tray are hot-swappable for carrier-class resiliency. The Cisco AS5350 Universal Gateway is the only access server in this form factor that offers universal port capability with these high-availability features.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco AS5350	• 2 to 8 channelized CT1/7 CE1/PRI compact and modular universal • High-performance modem, ISDN, and voice call termination • Universal port services (data, voice, fax)

Key Features

- 1 RU modular high-performance 2 to 8 channelized CT1/7 CE1/PRI system
- Universal Gateway—which supports multiple data, voice, and fax services on any port at any time
- Ideal for Tier 2/3 ISPs and enterprises requiring innovative universal services
- Feature cards: 2, 4, or 8 CT1/7 E1/PRI feature cards (ISDN calls terminated on the card); 60 or 108 channel Universal Port feature card
- Two 10/100BaseT autosensing Ethernet LAN ports
- Two 8 MB serial WAN ports for Frame Relay, HDLC, or PPP WAN backhaul
- Carrier Class Resiliency: All feature cards and fan tray are hot swappable, modem and voice DSP are pooled and can be configured as spares, AC internal power supply with dual fans, Redundant LAN/WAN backhaul ports, Thermal management and environmental monitoring, ETSI/NEBS Level 3 compliant
- Cisco SS7 signaling gateway interoperability

Competitive Products

- Lucent/Ascend: Max TNT
- 3Com/CommWorks: Total Control 1000
- Alcatel: 7505 Series
- Nuera: BTX Series
- Siemans: HiPath Series

Specifications

Feature	Cisco AS5350
Processor	250 MHz RISC processor
Memory	SDRAM: 128 MB (default), 512 MB (maximum) Shared Input/output (I/O): 64 MB (default), 128 MB (maximum) Boot Flash: 8 MB (default), 16 MB (maximum) System Flash: 32 MB (default), 64 MB (maximum) Layer 3 Cache: 2 MB
Feature Card Slots	Three slots
Egress Ports	Two 10/100-MB Ethernet ports Two 8-Mbps serial ports T1/E1 DS1 trunk feature cards
LAN Protocols	IP, IPX, AppleTalk, DECNet, ARA, NetBEUI, bridging, HSRP, 802.1Q
WAN Protocols	Frame Relay, PPP, HDLC (leased line)
Routing Protocols	RIP, RIPv2, OSPF, IGRP, EIGRP, BGPv4, IS-IS, AT-EIGRP, IPX-EIGRP, Next Hop Resolution Protocol (NHRP), AppleTalk Update-Based Routing Protocol (AURP)
QoS Protocols	IP Precedence, Resource Reservation Protocol (RSVP), Weighted Fair Queuing (WFQ), Weighted Random Early Detection (WRED), Multichassis Multilink PPP (MMP) fragmentation and interleaving, 802.1P
Access Protocols	PPP, Serial Line Internet Protocol (SLIP), TCP Clear, IPXCP, ATCP, ARA, NBFCP, NetBIOS over TCP/IP, NetBEUI over PPP, protocol translation (PPP, SLIP, ARA, X.25, TCP, local-area transport [LAT], Telnet), and Xremote
Bandwidth Optimization	Multilink PPP (MP), MLP, TCP/IP header compression, Bandwidth Allocation Control Protocol (BACP), bandwidth on demand, nonfacility-associated signaling (NFAS), traffic shaping
Voice Compression	G.711, G.723.1, (5.3K and 6.3K), G.726, G.729ab, G.Clear, GSM-FR
DSP Voice Features	Echo cancellation, programmable up to 128 ms Transparent transcoding between A-law and mu-law encoding Voice activity detection, silence suppression, comfort noise generation Fixed and adaptive jitter buffering Call progress tone detection and generation - Dial tone, busy, ring-back, congestion, and re-order tones with local country variants DTMF, Multifrequency (MF) Continuity Testing (COT)

Feature	Cisco AS5350
Voice and Fax Signaling Protocols	H.323v2, H.323/v3, H.323v4, SIP, MGCP 1.0, TGCP 1.0, Voice Extensible Markup Language (VoiceXML) Real-Time Streaming Protocol (RTSP), Extended Simple Mail Transfer Protocol (ESMTP) T.38 real-time fax relay T.37 fax store and forward Fax detection Fax and modem passthrough Open Settlements Protocol (OSP) Media Recording Control Protocol (MRCP) Text to Speech (TTS) Servers Automatic Speech Recognition (ASR) Servers
SS7	Integrated SLT functionality
Network Security	RADIUS or TACACS+ PAP or CHAP authentication Local user/password database DNIS, CLID, call-type preauthentication Inbound/outbound traffic filtering(including IP, IPX, AppleTalk, bridged traffic) Network Address Translation (NAT) Dynamic access lists SNMPv2, SNMPv3
Virtual Private Networking	IP Security (IPSec) Policy enforcement (RADIUS or TACACS+) L2TP, Layer 2 Forwarding (L2F), and generic routing encapsulation (GRE) tunnels Firewall security and intrusion detection QoS features (committed access rate [CAR], Random Early Detection [RED], IP Precedence, policy-based routing)
Channelized T1	Robbed-bit signaling; Loop Start, Immediate Start, and Wink Start Protocols
Channelized E1	CAS, PRI, E1 R1, E1 R2, leased line, Frame Relay, G.703, G.704
ISDN Protocols Supported	Sync mode PPP, V.120, V.110 at rates up to 38400 bps Network- and User-side ISDN NFAS with backup D-channel QSIG, Feature Group B, Feature Group D DoVBS
Modem Protocols Supported	V.90 or V.92 standard supporting rates of 56000 to 28000 in 1333 bps increments V.92 Modem on Hold V.44 Compression Fax out (transmission) Group 3, standards EIA 2388 Class 2 and EIA 592 Class 2.0, at modulations V.33, V.17, V.29, V.27ter, and V.21 K56Flex at 56000 to 32000 in 2000 -bps increments ITU-T V.34 Annex 12 at 33600 and 31200 bps and many others
Wireless Protocols Supported	V.110, V.120
Full Cisco IOS Support	IP Plus and Enterprise Plus feature sets
Console and Auxiliary Ports	Asynchronous serial (RJ-45)
Chassis	Dimensions (H x W x D): 1.75 x 17.5 x 20.5 in. Weight (fully loaded): 22 lbs. (10 kg)

Selected Part Numbers and Ordering Information[1]

Cisco AS5350 Universal (Data) System Bundles

AS535-2T1-48-AC	AC AS5350; 2T1, 60 ports, IP+ IOS, 48 Data Lic
AS535-4T1-96-AC	AC AS5350; 4T1, 108 ports, IP+ IOS, 96 Data Lic
AS535-8T1-192-AC	AC AS5350; 8T1, 216 ports, IP+ IOS, 192 Data Lic
AS535-2E1-60-AC	AC AS5350; 2E1, 60 ports, IP+ IOS, 60 Data Lic
AS535-4E1-120-AC	AC AS5350; 4E1, 120 ports, IP+ IOS, 120 Data Lic
AS535-8E1-210-AC	AC AS5350; 8E1,216 ports,240 ISDN ports, IP+ IOS,210 Data Lic

Cisco AS5350 Universal (Voice) System Bundles

AS535-2T1-48-AC-V	AC AS5350 Voice; 2T1, 60 ports, IP+ IOS, 48 Voice Lic
AS535-4T1-96-AC-V	AC AS5350 Voice; 4T1, 108 ports, IP+ IOS, 96 Voice Lic
AS535-8T1-192-AC-V	AC AS5350 Voice; 8T1, 216 ports, IP+ IOS, 192 Voice Lic
AS535-2E1-60-AC-V	AC AS5350 Voice; 2E1, 60 ports, IP+ IOS, 60 Voice Lic
AS535-4E1-120-AC-V	AC AS5350 Voice; 4E1, 120 ports, IP+ IOS, 120 Voice Lic
AS535-8E1-210-AC-V	AC AS5350 Voice; 8E1, 216 ports, IP+ IOS, 210 Voice Lic

Cisco AS5350 Spare Chassis

AS5350-AC=	AC 5350 Chassis with Motherboard, IP Plus IOS, default memory
AS5350-DC=	DC 5350 Chassis with Motherboard, IP Plus IOS, default memory

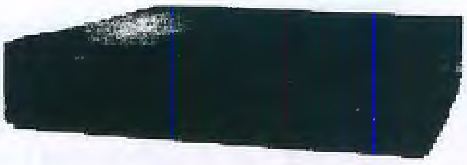
Cisco AS5350 Software	
S535AK8-12202XA	Cisco AS5350 Series IOS ENTERPRISE PLUS IPSEC 56
S535AP-12202XA	Cisco AS5350 Series IOS ENTERPRISE PLUS
S535CK8-12202XA	Cisco AS5350 Series IOS IP PLUS IPSEC 56
S535CP-12202XA	Cisco AS5350 Series IOS IP PLUS
Cisco AS5350 Memory Options & Spares	
MEM-UP1-AS535	16M Bootflash,64M System Flash,256M Main,128M Shared I/O Memory
MEM-16BF-AS535	AS5350 16MB Boot Flash upgrade
MEM-64F-AS535	AS5350 64MB System Flash upgrade
MEM-256M-AS535	AS5350 256MB Main SDRAM upgrade
MEM-128S-AS535	AS5350 128MB Shared I/O upgrade
Cisco AS5350 Spare DFC Boards	
AS535-DFC-2CT1=	AS5350 Dual T1/PRI DFC card
AS535-DFC-2CE1=	AS5350 Dual CE1/PRI DFC card
AS535-DFC-4CT1=	AS5350 Quad T1/PRI DFC card
AS535-DFC-4CE1=	AS5350 Quad E1/PRI DFC card
AS535-DFC-8CT1=	AS5350 Octal T1/PRI DFC card
AS535-DFC-8CE1=	AS5350 Octal E1/PRI DFC card
AS535-DFC-60NP=	AS5350 60 Nextport DFC card
AS535-DFC-108NP=	AS5350 108 Universal Port Card
Cisco AS5350 Spare Accessories	
AS5350RM-19/24=	AS5350 19/24 Rack Mount Kit, Spare
AS535-FTA=	AS5350 Fan Tray Assembly, Spare
AS535-AC-PWR=	AS5350 AC Power Supply, Spare
AS535-DC-PWR=	AS5350 DC Power Supply, Spare
AS535-DFC-CC=	AS5350 DFC Carrier Card

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco AS5350 Universal Gateway Web site: **http://www.cisco.com/go/as5350**

Cisco AS5400 Series Universal Gateways



Cisco AS5400 Series Universal Gateways offer unparalleled capacity in only two rack units (2RUs) and provides universal port data, voice and fax services on any port at any time. High-density (up to 1 CT3), low power consumption (7.2A at 48 VDC per CT3), and universal port digital signal processors (DSPs) make Cisco AS5400 Series Universal Gateways ideal for many network deployment architectures, especially colocation environments and mega points of presence (POPs).

The Cisco AS5400 Series consists of two models, the Cisco AS5400 and the Cisco AS5400HPX. The gateways share the same architecture; the primary difference is the processing capability of the two platforms. The Cisco AS5400 offers unparalled dial capacity and scalability for MLPPP, L2TP, and V.120 sessions, whereas the Cisco AS5400HPX provides enhanced performance for processor intensive voice and fax applications.

Cisco AS5400 Series support a wide range of IP-based value-added services such as high-volume Internet access, regional/branch-office connectivity, corporate virtual private networks (VPNs), mobile wireless solutions, long distance for Internet service providers (ISPs), international wholesale long distance, distributed prepaid calling, Signaling System 7 (SS7) interconnect, and enhanced voice services.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco AS5400HPX	• High densityin a small footprint (16 CT1/CE1 or 1 CT3) • Universal port services (data, voice, fax) • Enhanced performance for processor intensive voice and fax applications • Compact form factor—easy to add capacity as the network grows • Low power per port • High performance async/ISDN/VoIP/wireless • T.38 real-time fax relay, T.37 fax store and forward, fax detection,unified communications • Flexible redundant backhaulmethods
Cisco AS5400	• Async/ISDN/Wireless data to 1 CT3 • Universal port services (data, voice, fax) or voice only services to 16 CT1/CE1

Key Features

- The Industry's only 2RU, CT3-capable universal gateway on the market with hot-swappable cards, internal redundant power supply
- Universal Gateway which provides universal port data, voice, and fax services on any port at any time
- Feature cards: 8 or 16 CT1/CE1 feature cards; 60 or 108 channel Universal Port feature card; All feature cards and fan trays are hot-swappable
- Redundant 10/100 Ethernet ports and redundant 8 Mbps serial backhaul ports for Frame Relay, HDLC or PPP WAN Backhaul
- One fast console port for local administrative access; one auxiliary port for remote administrative access
- Redundant LAN/WAN backhaul ports
- ETSI/NEBS Level 3 compliant
- AC or DC power supply with dual fans
- Cisco SS7 signaling gateway interoperability

Competitive Products

- 3Com/CommWorks: Total Control C1000
- Alcatel: 7505 Series
- Lucent: Max TNT
- Siemens: HiPath Series

Specifications

Processor Type	Cisco AS5400HPX: 390-MHz RISC processor Cisco AS5400:250-MHz RISC processor
Calls Supported	Cisco AS5400HPX: Voice or universal port services - to 648 concurrent calls(to 20T1s/16E1s) or Remote access services - to 648 calls (to 1CT3/16E1s) Cisco AS5400: Voice or universal port services - to 480 concurrent calls (to 20T1s/16E1s) or Remote access services - to 648 calls (to 1CT3/16E1s)
SDRAM	256 MB (default), 512 MB (maximum)
Boot Flash	8 MB (default) 16 MB (maximum)
System Flash	32 MB (default) 64MB (maximum)
Layer 3 Cache	Cisco AS5400HPX: 8 MB Cisco AS5400:2 MB
Shared input/output (I/O)	64 MB (default) 128 MB (maximum)
Feature Slots	7
Trunk Feature Cards	8 T1/E1/PRI 1 CT3
DSP Feature Card	60/180 Universal ports
LAN Protocols	IP, IPX, AppleTalk, DECnet, ARA, NetBEUI, bridging, HSRP, 802.1Q
WAN Protocols	Frame Relay, PPP, HDLC (leased line)
Routing Protocols	RIP, RIPv2, OSPF, IGRP, EIGRP, BGPv4, IS-IS, AT-EIGRP, IPX-EIGRP, Next Hop Resolution Protocol (NHRP), AppleTalk Update-Based Routing Protocol (AURP
QoS Protocols	IP Precedence, Resouce Reservation Protocol (RSVP), Weighted Fair Queuing (WFG), Weighted Random Early Detection (WRED), Multichassis Multilink PPP (MMP) fragmentation and intelreaving, 802.1P
Access Protocols	PPP, Serial Line Internet Protocol (SLIP), TCP Clear, IPXCP, ATCP, ARA, NBFCP, NetBIOS over TCP/IP, NetBEUI over PPP, protocol translation (PPP, SLIP, ARA, X.25, TCP, LAT, Telnet), & XRemote
Bandwidth Optimization	Multilink PPP (MLPPP), TCP/IP header compression, Bandwidth Allocation Control Protocol (BACP), Bandwidth on demand,Traffic shaping

7973
A.

Voice Compression	G.711, G.723.1 (5.3K and 6.3K), G.726, G.729ab, G.Clear, GSM-FR
DSP Voice Features	G.168 echo cancellation, programmable up to 128 ms Transparent transcoding between A-law and mu-law encoding Voice activity detection, silence suppression, comfort noise, fixed and adaptive jitter buffering Call progress tone detection and generation—Diatone, busy, ring-back, congestion, and re-order tones, with local country variants Continuity Testing (COT) DTMF, MF
Voice and Fax Signaling Protocols	H.323v2, H.323v3, H.323v4, SIP, MGCP 1.0, TGCP 1.0, Voice Extensible Markup Language (VoiceXML), Real-Time Streaming Protocol (RTSP), Extended Simple Mail Transfer Protocol (ESMTP) T.37 fax store and forward T.38 real-time fax relay Fax detection Fax and modem passthrough Open Settlements Protocol (OSP) Media Recording Control Protocol (MRCP) Text to Speech (TTS) Servers Automatic Speech Recognition (ASR) Servers
SS7	Integrated SLT functionality
Network Security	RADIUS or TACACS+, PAP or CHAP authentication, local user/password database DNIS, CLID, call-type pre-authentication Inbound/outbound traffic filtering (includig IP, IPX, AppleTalk, bridged traffic) Network Address Translation (NAT) and Dynamic access lists SNMPv2, SNMPv3
Virtual Private Networking	IP Security (IPSec) and Policy enforcement (RADIUS or TACACS+) L2TP, Layer 2 Forwarding (L2F), and generic routing encapsulation (GRE) tunnels Firewall security and intrusion detection
Channelized T1	Robbed-bit signaling; loop start, immediate start, and wink start protocols
Channelized E1	CAS, E1 R1, E1 R2, leased line, Frame Relay, G.703, G. 704
ISDN Protocols Supported	Sync mode PPP, V.120, V.110 at rates up to 38400 bps Network- and User-side ISDN DoVBS QSIG NFAS with backup D-channel
Modem Protocols Supported	V.90 or V.92 standard supporting rates of 56000 to 28000 in 1333 bps increments V.92 Modem on Hold, Quick Connect V.44 Compression Fax out (transmission) Group 3, standards EIA 2388 Class 2 and EIA 592 Class 2.0, at modulations V.33, V.17, V.29, V.27ter, and V.21 K56Flex at 56000 to 32000 in 2000 bps increments ITU-T V.34 Annex 12 at 33600 and 31200 bps and many others
Wireless Protocol	V.110, V.120
Full Cisco IOS Support	IP Plus and Enterprise Plus feature sets
Console and Auxiliary Ports	Asynchronous serial (RJ-45)
Chassis Dimensions (H x W x D)	3.5 x 17.5 x 18.25 in.
Chassis Weight (fully loaded)	35 lb maximum (15.8 kg)

For More Information

See the Cisco AS5400 Universal Gateways Web site: **http://www.cisco.com/go/as5400**

Cisco AS5850 Universal Gateway

The Cisco AS5850 Universal Gateway is a high-density, carrier-class gateway, offering unparalleled capacity and high availability. The Cisco AS5850 is specifically designed to meet the demands of large, innovative service providers, supporting up to five channelized T3s (CT3s), 96 T1s or 86 E1s of data, voice, and fax services on any port at any time. It offers high availability features such as hot-swap on all cards, load-sharing and redundant hot-swappable power supplies, redundant route processing cards and call admission control to ensure 99.999-percent availability.

The Cisco AS5850 supports a wide range of IP-based value-added services such as high-volume Internet access, corporate virtual private networks (VPNs), long distance for Internet service providers (ISPs), international wholesale long distance, distributed prepaid calling, Signaling System 7 (SS7) interconnect, and managed voice services such as hosted IP telephony, managed IP-PBX, multiservice VPNs, and IP contact centers.

Using the rich set of Cisco IOS Software features and Signaling System 7 (SS7) interconnection, service providers can quickly provision their network for new services to meet the rapidly changing demands of the communications provider marketplace.

As a highly flexible voice gateway, the Cisco AS5850 supports any coder-decoder (CODEC) at 100-percent capacity simplifying network engineering. An open programmable architecture streamlines rapid voice service creation with H.323, Session Initiation Protocol (SIP) or Media Gateway Control Protocol (MGCP).

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco AS5850	• Supportingup to 5 x CT3s, 96 T1s or 86 E1s of multiple data, voice, and fax services on any port at any time • Service provider or IP-focused installations • Highly available single system with multiple redundancy • Wholesale dial/voice, retail dial/voice, TDM grooming or wireless applications

Key Features

- High scalability—up to 3360 ports in a 14 RU chassis and provides for 6 times growth in same chassis
- Hot-swap redundant power supplies and power feeds
- Redundant DSPs and RSC
- Thermal/Power management and redundant fans
- DSP Resource Recovery Feature
- Supports H.323v2, H.323v3, H.323v4, SIP and MGCP 1.0
- Application-specific support including AOL and Prodigy traffic
- WAN optimization including routing filters, snapshot routine, dial-on-demand routing ASAP
- ETSI/NEBS Level 3 compliant
- Cisco SS7 signaling gateway interoperability

Competitive Products

- 3Com: TC 2000
- Lucent: APX 8000
- Siemens: HiPath Series
- Alcatel: 7505 Series

Specifications

Feature	Cisco AS5850
Slots	12 feature boardslots 2 RSC slots
Processor Type	266 MHz RISC processor plus 2MB of L3 cache SDRAM
RSC Switch Fabric	5 GBps, Layer 3 / 4 switching
Memory	512 MB SDRAM with ECC per RSC 128 MB SDRAM (with parity) perfeature card
Trunk Cards	Single CT3 plus216 DSP Channelfeature card 24 CE1/CT1 feature card G.703, G.704
Universal Port Card	324 Channel DSP-feature card
Egress Ports	Dual Gigabit load-balanced redundant Ethernetports with GBIC interfaces for user traffic One 10/100-Mbps Ethernet port with RJ45 connector for managementtraffic
LAN Protocols	IP
Service Support	Port Policy Management andSS7/C7
Routing Protocols	RIP, RIPv2, OSPF, IGRP, EIGRP, BGPv4, IS-IS, Next Hop Resolution Protocol(NHRP)
Access Protocols	PPP, Serial Line Iternet Protocol (SLIP), TCP Clear
Bandwidth Optimization	Multilink PPP (MLPPP), TCP/IP header compression, Bandwidth Allocation Control Protocol (BACP), Bandwidth on demand, Nonfacility-associated signaling (NFAS),traffic shaping
Network Security	RADIUS or TACACS+, PAP or CHAP authentication, local user/password database,DNIS, CLID, call-type pre-authentication, Inbound/outbound traffic filtering (including IP), SNMPv2, SNMPv3
Virtual Private Networking	IP Security (IPSec) and Policy enforcement (RADIUS or TACACS+), L2TP, Layer 2 Forwarding (L2F), and generic routing encapsulation(GRE) tunnels, Firewall security andintrusion detection, IP Precedence, policy-based routing
Channelized T1	PRI, robbed-bit signaling; loop start, immediate start, and wink start protocols
Channelized E1	CAS, E1 R2, PRI
ISDN Protocols	Sync mode PPP, V. 120, V. 110 at rates up to 38400
Voice Protocols	G.711, G.723.1, , G.726, G.729ab, G.Clear, GSM-FR H.323v2, H.323v3, H.323v4, SIP, MGCP 1.0 ECAN up to 128ms T.38 real-time fax relay Fax detection Fax and modem passthrough
Modem Protocols	V.90 or V.92 standard supporting rates of 56000 to 28000 in 1333-bps increments V.44 supporting increased throughput bymore than 100 percent for Internet browsing Fax out (transmission) Group 3, standardsEIA 2388 Class 2 and EIA 592 Class 2.0, at modulationsV.33, V.17, V.29, V.27ter, and V.21 K56Flex at 56000 to 32000 in 2000-bps increments ITU-T V.34 Annex 12 at 33600 and 31200 bps and more
ISDN Protocols	Sync mode PPP, V.120, V.110 at rates up to 38400 bps
Wireless Protocol	V.110
Console and Auxiliary Ports	Asynchronous serial (RJ-45)
Chassis Dimensions (HxWxD)	24.5 x 17.5 x 24 in.
Chassis Weight	220 lb (100 kg)

For More Information

See the Cisco AS5850 Web site: **http://www.cisco.com/go/AS5850**

Remote Dial Access Network Management Products

Universal Gateway Manager (UGM)

Network management applications and tools are critical for the successful deployment and operations of voice or data services. The Cisco Universal Gateway Manager (UGM) is an element management system for Cisco AS5000 Universal Gateways. The Cisco UGM enables network operators and administrators to efficiently deploy, manage and maintain Cisco AS5000 Universal Gateways supporting Voice over IP, managed voice, PSTN gateway, and dial access services.

Key Features

- Enables the efficient deployment and configuration of Cisco AS5000 Universal Gateways
- Monitors the operational status of Cisco AS5000 Universal Gateways and their subcomponents so that corrective action can be taken quickly
- Supports the rapid reconfiguration of Cisco AS5000 Universal Gateways for network or service changes
- Collects and presents a wide range of performance-related statistics for monitoring gateway and network efficiency
- Co-resides with Cisco MGC Node Manager (MNM) for Cisco PGW 2200 PSTN Gateway node management
- Provides interfaces to support its integration with existing network management applications

For More Information

See the Cisco Universal Gateway Manager Web site: **http://www.cisco.com/go/ugm**

Cisco Universal Gateway Call Analyzer

The Cisco Universal Gateway Call Analyzer (UGCA) tool monitors and troubleshoots Cisco AS5000 universal gateways that support dialup services. The Cisco Universal Gateway Call Analyzer complements other network management system (NMS) applications, adding call-level analysis capabilities that are not available with standard NMS applications.

Maintaining high call-success rates and quality connections are key challenges for any dial service provider. These metrics directly affect customer satisfaction and are fundamental indicators of network performance and efficiency. Numerous issues may cause service degradation, which may be rapid or may occur slowly. While public switched telephone network (PSTN) issues are frequently the source of problems, they are especially difficult to identify.

Cisco AS5000 universal gateways collect the detailed call-characteristic data needed to detect and diagnose issues that affect service. The Cisco Universal Gateway Call Analyzer is the window into this data, providing analysis and reporting features through an intuitive Web interface.

For More Information

See the Cisco Universal Gateway Call Analyzer Web site:
http://www.cisco.com/go/ugca

Cisco Resource Policy Management System

Wholesalers face a challenge when delivering service level agreements (SLAs) on a common network, especially when providing a range of services for different customers. The Cisco Resource Policy Management System (RPMS) is a software tool that provides policy management of platform resources. With Cisco RPMS, wholesalers are able to offer a variety of services to a variety of customers on a single set of gateways. Cisco RPMS offers not only effective resource management but the capability to build and deliver flexible service models that fit customers' unique requirements. Cisco RPMS can grow to support a wholesaler's changing needs, scaling as the network expands and delivering the services that customers demand, including wholesale dial, access to virtual private network (VPN) services.

Selected Part Numbers and Ordering Information[1]

Resource Policy Management System	
FR5X-PM-LIC	Port management licensefor 1 port (includesResource Pool Manager Call Tracker)
CRPMS-2.0	Cisco Resource Pool Manager Server v2.0 (1 server)
CRPMS-2s-2.0	Cisco Resource Pool Manager Server v2.0 (2 servers)
CRPMS-6S-2.0	Cisco Resource Pool Manager Server v2.0 (6 servers)
CRPMS-UPGRADE-2.0	Single Server Upgrade License from RPMS 1.x to version 2.0

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco Universal Gateway Manager: **http://www.cisco.com/go/ugm**
See the Resource Pool Manager Web site: **http://www.cisco.com/go/rpms**

SS7 Signaling & Softswitch Products

Cisco AS5x00 series products interoperate with various SS7 and Softswitch products, including the Cisco SC2200 Signaling Controller, the Cisco PGW 2200 Softswitch and the Cisco BTS 10200 Softswitch.

Cisco SC2200 Signaling Controller

Please see PGW 2200 Softswitch.

Cisco PGW 2200 Softswitch

The Cisco PGW 2200 provides the signaling and call control functionality that enables service providers (SPs) to bridge the boundary between the legacy PSTN and today's new world packet networks. Combined with Cisco's award winning media gateways, the PGW 2200 is the catalyst for PSTN Gateway solutions enabling dial offload, transit, business voice, H.323 and SIP based applications. The PGW 2200 leverages its protocol library of 90+ SS7/C7 variants to enable interconnect worldwide. In signaling mode the PGW adds SS7/C7 to the AS5X00 gateways, giving service providers around the world a proven cost-saving and reliable solution for connecting VoIP and Internet Dial Access solutions to the PSTN. SS7 signaling allows service providers to enter into new markets, optimize their networks for both voice and data traffic, and save drastically on monthly interconnect fees.

Cisco BTS 10200 Softswitch

The Cisco BTS 10200 Softswitch provides call-control intelligence for establishing, maintaining, routing, and terminating voice calls. The Cisco BTS 10200 Softswitch also serves as an interface to enhanced service and application platforms. Leveraging the power of packet networks while seamlessly operating with legacy circuit switched infrastructures, the Cisco BTS 10200 Softswitch empowers service providers and carriers to gracefully transition to packet-based technology. Implementing the Cisco BTS 10200 Softswitch ensures rapid service deployment, carrier-grade reliability, service flexibility, scalability to millions of subscribers, and cost savings through investment optimization and operational efficiencies.

For More Information

See SS7 Signaling & Softswitch Products Web site:
http://www.cisco.com/en/US/products/hw/vcallcon/index.html

Additional Remote Dial Access Products

- In addition to the AS5350/AS5400/AS5850 series access gateways, the Cisco 2600/3600 series routers (see pages 1-16 and 1-22) also support dial-up, data, and voice access via network and modem modules, and voice interface cards
- For sites that require access via multiple external analog modems, the AS2509/AS2511-RJ access servers (see page 1-14) and 2600 series routers (see page 1-16) are ideal for low-density, dial applications
- For small office ISDN connectivity, see Cisco 800 series routers (see page 1-9)

Cisco uBR7100 Series Universal Broadband Router

The Cisco uBR7100 Series is a complete, compact, easy-to-use product that enables cost-effective, high-speed Internet access in the hospitality multidwelling (MDU) and multitenant (MTU) market space using the coaxial cable already in a building. The product requires exceptionally low capital investment and minimal setup time to provide online Internet access and support residential voice services. For Tier 2 or Tier 3 cable operators, it is the industry's most cost-effective, feature-rich CMTS and integrated router. The Cisco uBR7111 and Cisco uBR7114 models are CableLabs qualified to DOCSIS 1.0 specifications. The Cisco uBR7111E and Cisco uBR7114E models are tComLabs qualified to EuroDOCSIS 1.0 specifications. The Cisco uBR7111 and Cisco uBR7111E contain one downstream port and one upstream port. The Cisco uBR7114 and Cisco uBR7114E contain one downstream port and four upstream ports. All models support bidirectional or telco-return traffic.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco uBR7100 Series	• For MxU customers: the Cisco uBR7100 Series enables high-value Internet and residential voice services over a DOCSIS or EuroDOCSIS cable infrastructure • For cable operators: the Multi-tenant/dwelling Unit (MxU) market represents an untapped opportunity to expand broadbandcable service. Given the small subscriber base of a typical MxU setting, the challenge has been to deliver robust services quickly and cost-effectively for an accelerated break-even point and a quicker return on investment—enabled by the Cisco uBR7100 Series

Key Features

- Complete package that includes a combined router and CMTS with an integrated upconverter, and embedded Network Interface
- Standards-based: DOCSIS 1.0 and DOCSIS 1.1-based; EuroDOCSIS models available
- Reliable operation to ensure the system remains online
- Uses Cisco IOS Software

Specifications

Feature	Cisco uBR7111 and uBR7114	Cisco uBR7111E and uBR7114E
Memory	Flash: 48 MB; System: 128 MB	Flash: 48 MB; System: 128 MB
Line Card with Integrated Upconverter (Cable Plant Interface)	uBR7111: 1 downstream and 1 upstream uBR7114: 2 downstream and 4 upstreams	uBR7111E: 1 downstream and 1 upstream uBR7114E: 2 downstream and 4 upstreams
Integrated Upconverter	DOCSIS Annex B, 6 MHz High level output =+61dBmV, 55 to 858 MHz Optimized for 64 and 256 QAM	DOCSIS Annex A, 8 MHz, High level output: = +61 dBmV, 55 to 858 MHz Optimized for 64 and 256 QAM
Port Adapter (WAN or backbone Interface)	Embedded dual 10/100 BaseT Ethernet (TX FE) provided Supports one addtional PA; options include the following using Cisco IOS Release12.1(8)EC minimum: Ethernet: • PA-4E-4-port Ethemet 10BASE-T • Fast Ethernet: • PA-FE-TX-1-port 100BASE-TX Fast Ethernet • PA-FE-FX-1-port 100BASE-FX Fast Ethernet • PA-2FE-TX 2-port 100BASE-TX Fast Ethenet • PA-2FE-FX 2-port 100BASE-FX Fast Ethernet Serial: • PA-MC-4T1 4-port multichannelT1 Port Adapter with integrated CSU/DSUs • PA-MC-2T1 2-port multichannelT1 Port Adapter with integrated CSU/DSUs • PA-E3-1-port E3 serial Port Adapter with E3 DSU • PA-T3-1-port T3 serial Port Adapter with T3 DSU • PA-2E3-2-port E3 serial Port Adapter with E3 DSUs • PA-2T3-2-port T3 serial Port Adapter with T3 DSUs • PA-4T+-4-port serial Port Adapter, enhanced • PA-4E1G-75-4-port E1-G.703 serial Port Adapter (75-ohm/unbalanced) • PA-4E1G-120-4-port E1-G.703 serial Port Adapter (120-ohm/balanced) HSSI: • PA-2H-2-port HSSI • ATM: • PA-A3-8T1IMA, 8-port ATM inverse T1 multiplexer Port Adapter • PA-A3-OC3SML—1-port OC-3c ATM, PCI-based single-mode long reach port adapter • PA-A3-OC3MM, 1-port ATM enhanced OC3c/STM1 multimode Port Adapter • PA-A3-OC3SMI—1-port OC-3c ATM, PCI-based single-mode intermediatereach port adapter POS: • PA-POS-OC3SMI, 1-port Packet/SONET OC3c/STM1 single-mode Port Adapter	Same as Cisco uBR7111 and Cisco uBR7114

Feature	Cisco uBR7111 and uBR7114	Cisco uBR7111E and uBR7114E
Power Options	Single; 100 to 240 VAC input voltage	Single; 100 to 240 VAC input voltage
Minimum Cisco IOS Software Release	12.1(5)ECI minimum	12.1(7)EC minimum

For More Information

See the Cisco uBR7100 series Web site: **http://www.cisco.com/go/ubr7100**

Cisco uBR7246VXR Universal Broadband Router

The Cisco uBR7246VXR-a member of the Cisco uBR7200 Series-combines the functionality of a CMTS with an advanced router. The Cisco uBR7246VXR provides a single, multiservice, scalable platform that gives cable companies and ISPs the ability to deliver IP data and VoIP services to DOCSIS or EuroDOCSIS-compliant cable modems and set-top boxes. The Cisco uBR7246VXR is CableLabs qualified to DOCSIS 1.1, as well as PacketCable 1.0 specifications. The product is also tComLabs qualified to EuroDOCSIS 1.1 specifications.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco uBR7246VXR	• Positioned for high-growth cable deployments • Flexible port expansion for multiservice deployment options • Supports up to 8,000 subscribers per chassis with 3.2 Gbps back plane • 4 line card slots, 2 port adapter slots, 1 I/O controller slot, 1 NPE slot, and 1 clock card slot for VoIP

Key Features

- Standards-based—Supports DOCSIS/EuroDOCSIS 1.0 and DOCSIS 1.1
- Modularity allows for customized configuration per plant characteristics for optimization of topology and network bandwidth
- Cisco IOS Software—Delivers proven stability and offers advanced features such as multiprotocol routing, tunneling, bandwidth management, QoS, guaranteed service levels, service-level monitoring and many CPE management options
- Ease of management and upgrades—Supports online insertion and removal of components to allow seamless upgrades of port adapters, line cards, and power supplies without service interruption. Provides single, centralized point of administration for remote devices

Specifications

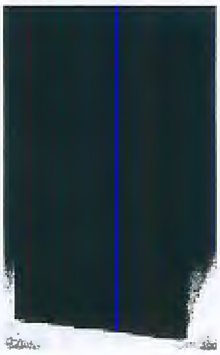
Feature	Cisco uBR7246VXR
Cable Line Cards and Number of Slots	4
Supported cable line cards (Cable Plant Interfaces)	uBR-MC14C; uBR-MC16C; uBR-MC16E; uBR-MC16S; uBR-MC28C
Port Adapter Slots (LAN/WAN interfaces)	2
Supported PA categories	Ethernet: Fast Ethemet; Gigabit Ethernet Serial (V.35, E1-G.703/G.704, T3/E3) Serial Multi-channel T1 HSSI ATM T3/E3 ((PCI-based) ATM OC-3c (PCI-based) POS OC-3c DPT OC-12c/STM4c
Power Supply Shots	2
Power Supply Option	AC; Dual AC; DC; Dual DC

Feature	Cisco uBR7246VXR
Input/Output (I/O) controller	uBR7200-I/O uBR7200-I/O-FE uBR7200-I/O-2FE/E
I/O flash options for PCMCIA slots	Flash disk (48 MB) Flash disk (128 MB)
Network processing engines (NPE)	uBR7200-NPE-G1,NPE-400, and NPE-225
Add-on processor memory options	SDRAM (128 MB, 256 MB) for NPE-225 only SDRAM (128 MB, 256 MB = 512 MB) for NPE-400 only 1 GB, 512 MB, 128 MB for uBR7200-NPE-G1
Router Bandwidth	3.2 Gbps

For More Information

See the uBR7200 Web site: **http://www.cisco.com/go/ubr7200**

Cisco uBR10012 Universal Broadband Router



The Cisco uBR10012 Universal Broadband Router is a new class of CMTS, that handles the volume, capacity, and complexity of large cable headends or distribution hubs. It combines the revenue-generating features and stability of the market-leading Cisco uBR7200 Series with an architecture that is optimized for aggregation and virtually limitless future growth. The Cisco uBR10012 goes beyond the traditional "carrier class" definition, to deliver the highest level of service availability and capacity of any production CMTS available today. It employs a mix of distributed, centralized, and parallel processing to enable consistently high, real-world performance. The Cisco uBR10012 is CableLabs qualified to DOCSIS 1.0 and DOCSIS 1.1 specifications. The product is also tComLabs qualified to EuroDOCSIS 1.0 specifications.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco uBR10012	• High-end throughput, capacity, and service handling for a mix of IP data, voice, and video services over cable—supporting a wide variety of applications, media, session types, subscriber profiles, and access devices • Support for advanced feature sets, varying QoS requirements, service-level differentiations, and transport strategies (MPEG, IP, multicast, unicast, broadcast) that include implementing flow control to various cable CPE devices

Key Features

- Highest-capacity CMTS that leverages the proven stability of the industry-standard Cisco uBR7200 Series, the highly scalable architecture of the Cisco 10000 Internet Router, and feature-rich Cisco IOS Software
- Multiservice support, optimized to provide high throughput and accelerated processing using PXF technology; exceptional throughput on each connection in the chassis is achieved
- Standards-based design, support includes DOCSIS 1.0 and DOCSIS 1.1
- Reliability—Designed to eliminate single points of failure and allow technicians to swap out cards online; architected to provide redundancy throughout the system that includes redundant processing engines, bus interconnects, and power supplies

- Secure, scalable choices protect your investment and ensure current and future business growth can be accommodated; the architecture supports planned system and network expansion, including scaling IP services forwarding capacity, increasing connection speeds and densities, and extensive route scaling techniques

Specifications

Feature	Cisco uBR10012
Modular Slots	8 slots for cable line cards 4 slots for LAN/WAN interfaces 2 slots for Performance Routing Engines(PREs) 2 slots for Timing Communication and Control Plus (TCC+) modules
Supported Cards	Cable line cards that include: CiscouBR line cards with a Cisco Line Card Processor (LCP2) and Cisco 5X20 BPE Timing, Communications, and Control Plus(TCC+) card Gigabit Ethernet (GE) netwok uplink card OC-12 Packet Over SONET (POS) networkuplink card OC-48 DPT Interface
Processor Type	Parallel Express Forwarding (PXF)
Flash Memory	48 MB (default); 128 MB (maximum)
DRAM Memory	512 DRAM (default)
Software Supported	Minimum software requirement: Cisco IOS Software Release 12.2(11)BC1 minimum for the Cisco 5X20 BPE, Cisco IOS Software Release 12.2(13)BC minimum for the Cisco OC-48 DPT Interface
Power Supply	DC, AC
Hot-Swappable	Yes
Backplane Capacity	51.2 Gbps
Physical Dimensions (H x W x D)	Height: 31.25 in. (79.4 cm)—18 rack units (RU) Width: 17.2 in. (43.7 cm) Depth: 22.75 in. (57.8) Mounting: 19 in. rack mountable (front or rear), 2 units per 7 ft. rack Note: Mounting in 23 in. racks is possible with optional third-party hardware
Weight	Weight: 235 lb (106.6 kg) fully configured chassis

For More Information

See the Cisco uBR10012 Web site: **http://www.cisco.com/go/ubr10012**

Cisco RF Switch

The Cisco RF Switch works with the Cisco uBR10002 and uBR7246VXR Universal Broadband Router to provide a fully redundant DOCSIS system that enables cable service providers to achieve PacketCable system availability, minimize service disruptions, and simplify operations. The Cisco RF Switch is part of Cisco's newest high-availability N+1 solution set. In combination with the Cisco uBR10012 and uBR7246VXR, the Cisco RF Switch enables a fully redundant CMTS with no single point of failure. The product maximizes density with more than 250 MCX-type connectors that interface the Cisco uBR10012 and the cable plant. The Cisco RF Switch contains RF combiners/splitters, RF switch logic, and RF switch drivers. The product offers ten upstream switch modules, three downstream switch modules, an Ethernet controller module, an AC or DC power supply, and color coding, preterminated cabling.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco RF Switch	As cable service providers enter the VoIP market, high availability (24x7 service) for broadband cable IP services is becoming a requirement. The Cisco RF Switch enables cable service providers to achieve PacketCable system availability, minimize service disruptions, and simplify operations.

Key Features

- Front-panel serviceability with module Hot Swap capability that eliminates downtime for RF paths
- Modular upstream and downstream capacity with ten upstream, three downstream, and one blank slot that optimizes the serviceability of the CMTS; each of the 14 modules represent a port on a cable line card. Each switch module contains seven working or "active" inputs, plus one protect or "standby" input and seven protected outputs. Inputs are connections from the Cisco uBR10012 and uBR7246VXR to the Cisco RF Switch. Outputs are connections from the Cisco RF Switch to the HFC plant
- Fully passive working path; hardware components do not affect data and VoIP services
- Active components only in protect path; servicing of protect cards offer no disruption to data and VoIP services
- Position-sensing latching relays; robust design maintains operation during power disruptions
- Flexible, external design with more than 250 connectors—unmatched port density
- N+1 redundancy

7962
A.

Specifications

Feature	Cisco RF Switch
Input Power Requirements	• AC: 100 to 240 VAC, 50 or 60 Hz, operating range: 90 to 254 VAC • DC: -48 to -60 VDC, operating range: -40.5 to –72 VDC, 200 mVpp ripple/noise
Environmental	• Operational temperature range: 0 to +40°C • Operating temperature range: -5 to +55°C
Unit Control	• 10BaseT Ethernet—SNMP • Switching time from active (working) to standby (protect): 150 mS maximum after SNMP command • Cisco uBR10012 and uBR7246VXR
Connectors	• RF connectors: MCX • AC power: IEC320 type • DC power: Three terminal block • Ethernet: RJ-45 • RS-232 Bus: 9-pin male D
Reliability	• 41,000 MTBF @ +50°C as calculated by Bellcore 5, 80 percent confidence factor
Physical	• Dimensions (H x W x D): 19 x 15.5 x 5.25 in. (842 x 384 x 132 mm) • Weight: 36 lbs
Input Power Requirements	• AC: 100 to 240 VAC, 50 or 60 Hz, operating range: 90 to 254 VAC • DC: -48 to -60 VDC, operating range: -40.5 to –72 VDC, 200 mVpp ripple/noise

Feature	Cisco RF Switch
Environmental	• Operational temperature range: 0 to +40°C • Operating temperature range: -5 to +55°C
RF requirements	• Input/output impedance: 75 ohms • Maximum RF input power: +15 dBm (63.75 dBmV) • Switch type: Electro-mechanical, absorptive for working path, non-absorptive on the protect path • Switch setting time per switch module: 20 ms maximum • Downstream frequency range: 54 to 860 MHz • Typical downstream insertion loss: +/-1.1 dB from CMTS to cable plant; +/- 2.1 dB from protect to cable plant; 5.5 dB from working to output; 8.0 dB from protect to output • Downstream insertion loss flatness: +/- 1.1 dB from CMTS to cable plant; +/- 2.1 dB from protect to cable plant • Downstream output return loss: >15.0dB at <450 MHz, > 12.0 dB at >= 450 MHz • Downstream input return loss: >15.0 dB • Downstream isolation: > 60 dB from channel to channel in working mode; > 52 dB from CMTS to protect when in protect mode • Upstream frequency range: 5 to 70 MHz • Typical upstream insertion loss: 4.1 dB from cable plant to CMTS; 5.2 dB from cable plant to protect • Upstream insertion loss flatness: +/- 0.4 dB from cable plant to CMTS, +/- 0.6 dB from cable plant to protect • Upstream input return loss:> 16 dB • Upstream isolation: > 60 dB from channel to channel in working mode; > 60 dB from CMTS to protect when in protect mode • Protect mode: CMTS return loss >10 dB, cable plant return loss: >10dB

For More Information

See the Cisco RF Switch Web site: **http://www.cisco.com/go/rfswitch**

Broadband Cable—Customer Premise Equipment (CPE)[1]

Cisco uBR900 Series Cable Access Routers

The Cisco uBR900 Series Cable Access Routers provide commercial services for cable operators, allowing them to expand their broadband service offerings. Both the Cisco uBR905 and Cisco uBR925 support IP data transmission over a cable plant and offer hardware-accelerated IPSec VPN support.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco uBR905 Cable Access Router	• Data-only broadband services (or voice separately via Ethernet) • High-speed, secure remote tunneling via hardware accelerated IPSec VPN
Cisco uBR925 Cable Access Router	• Two voice (VoIP) connections via RJ-11 ports • Data broadband services, router functionality, and VPN support • Easy-to-manage solution for telecommuters and small offices

[1] Cisco VoIP Residential CPE Partner Program—To help drive deployment of residential VoIP services to market, Cisco offers a program that identifies low-cost residential VoIP modems that have passed interoperability testing with Cisco. Cable service providers should contact their sales representatives for vendors, models, pricing and volume discount opportunities.

Key Features

- Integrated high-speed cable modem and router that operates with any DOCSIS 1.1 or DOCSIS 1.0-compliant CMTS; both Cisco uBR900 Series models are DOCSIS 1.1-ready
- Integrated Cisco IOS Software router, cable modem, and four-port Ethernet hub that offers advanced networking capabilities and investment protection

Specifications

Feature	Cisco uBR905	Cisco uBR925
Ports	4-port 10Base-T Ethernethub 1-port console 1-port CATV (Female F Connector)	4-port 10Base-T Ethernet hub 1-port USB 2 ports RJ-11 1-port console 1-port CATV
Routing Features	NAT/PAT, DHCP Server	Same as Cisco uBR905
Security Features	56-bit IPSec 3DES IPSec optional IPSec hardware acceleration Firewall optional	Same as uBR905
Voice Support	No	Yes

For More Information

See the uBR900 series Web site: **http://www.cisco.com/go/ubr900**

Remote Cable Access—Network Management Products

Cisco Cable Manager

Cisco Cable Manager is a client/server application that helps cable service providers deploy, maintain, monitor and troubleshoot cable equipment on an HFC network. The product manages DOCSIS and EuroDOCSIS-compliant CMTS and CPE, providing both operations center visibility, as well as technician access.

Cisco Cable Diagnostic Manager

Cisco Cable Diagnostic Manager is a web-based tool to help Customer Service Representatives at cable companies better handle subscriber calls and determine where problems reside in the network. Cisco Cable Diagnostic Manager provides status summary for the network neighborhood and fiber node, status on the DOCSIS or EuroDOCSIS-certified cable modem, as well as status on the Cisco CMTS products: Cisco uBR10012, uBR7200 Series, and uBR7100 Series.

Cisco Broadband Troubleshooter

Cisco Broadband Troubleshooter provides an efficient tool to help network operations center (NOC) personnel and field technicians detect, diagnose, and isolate problems between the cable plant and connected DOCSIS CPE devices. The product allows a technician to characterize upstream and downstream trouble patterns and quickly identify "flapping" CPE devices that are experiencing persistent connectivity problems. Operators can quickly discern CPE connectivity impairments by identifying noise, attenuation, provisioning, and packet-corruption issues.

Cisco Broadband Configurator

Cisco Broadband Configurator is a GUI-based tool designed to collect information needed to generate and download configuration files for DOCSIS or EuroDOCSIS cable modems and set-top boxes. There are two versions of the tool: a free, web-based version accessible via Cisco.com, and a stand-alone Java-based desktop version. Cisco Broadband Configurator enables point and click configuration of CPE values for RF, class of service, vendor information, SNMP parameters, BPI, TFTP, telco-return attributes, and CPE data.

For More Information

See the Cable Manager Web site: **http://www.cisco.com/go/cablemgr**
See the Cisco Cable Troubleshooter Web site:
http://www.cisco.com/go/troubleshooter

DSL Remote Access—Customer Premise Equipment (CPE)

Cisco offers the industry's broadest array of business-class DSL (G.SHDSL and ADSL) CPE solutions, from Enterprise to branch office, to Small Office/Home Office (SOHO) applications. Cisco's CPE solutions offer the choice of key features including Firewall, VPN, and Voice-over DSL support. And, Cisco's industry leading IOS-based capabilities enable QoS, policy management, and standardized set-up and configuration. Cisco CPE Products include:

- Cisco SOHO Series Ethernet, ADSL over ISDN, ADSL and G.SHDSL RoutersRouters (page 1-8)
- Cisco 800 Series Routers (page 1-9)
- G.SHDSL WAN Interface Cards (WICs) for 1700, 2600/2600XM, 3600 Series (see Chapter 1: Routers)
- Cisco IAD 2400 Series (w/G.SHDSL) (page 4-21)

Broadband Services Aggregation

The Cisco broadband aggregation portfolio includes the Cisco 6400 Broadband Aggregator, Cisco 7200 Series Router, the Cisco 7400 Series Internet Router, and the Cisco 10000 Series Internet Router. This portfolio covers all possible broadband aggregation markets. The Cisco 6400 and Cisco 10000 Series routers are carrier class broadband aggregation routers designed to provide high-density, high-performance services while maintaining the high-availability standards of large-scale carrier deployments. The Cisco 7200,Cisco 7301and Cisco 7400 Series routers cover the ISP and retail space by providing a dense, feature-rich platform but only taking a small footprint in the network.

- Cisco 7400: Highest density PPP aggregation per rack-unit
- Cisco 7301: Highest Density PPP aggregation per rack-unit
- Cisco 7200: Most versatile platform
- Cisco 6400: Only platform offering ATM switching and broadband aggregation
- Cisco 10000: Highest availability on a carrier-class integrated edge router

With this portfolio, Cisco can address the broadest set of requirements in terms of form factor, density, performance and scale, and offer customers a unique level of choice, with products optimized for any customer deployment.

Cisco 7200 Series

When ordered with the Cisco IOS 7200 Series Broadband User Services License (part number FR-BUS72), the 7200 delivers scaled PPP, RBE, and L2TP sessions and tunnels in addition to rich IP services. It enables service providers to provision broadband Internet access and supports all of the popular access technologies deployed today, including DSL, Cable, Wireless, and Dial Access. It is ideal for medium-density applications and is capable of handling up to 16000 subscribers in a single chassis. The 7200 is a modular platform with a choice of processing engines and a wide variety of WAN and LAN port adapters, including T1/E1, DS3, OC-3, Fast Ethernet, and Gigabit Ethernet. See page 1-31 for more information on the 7200 series.

Cisco 7301 Series

When ordered as 7301-BB-8K and 7301-BB-16K the Cisco 7301 Series Router provides a compact, high-performance single-rack-unit (1RU) router coupled with a broad set of interfaces and Cisco IOS® Software features, which makes it ideal for Broadband applications. The Cisco is capable of handling up to 16,000 simultaneous sessions and allowing for a pay-as-you-grow "rack and stack" architecture.

Cisco 7400 Series

When ordered as a part number 7401ASR-BB, the 7400 series provides high-performance broadband services aggregation like the 7200, but in a low-power one rack unit (1 RU) form factor. It offers one port adapter (PA) slot supporting over 40 standard 7200 series PAs, including T1/E1, DS3, OC-3, Fast Ethernet, and Gigabit Ethernet; making it ideal for small- and medium-density applications. See page 1-38 for more information on the 7400 series.

Cisco 10000 Series

With recent enhancements, the Cisco 10000 is the industry's only integrated edge router that delivers highly available, line-rate performance without compromises for service providers deploying IP services to broadband, leased line, ATM, and frame relay customers. With 99.999 percent uptime, the platform delivers high-performance broadband features including support for 32,000 (61,500 in the future) broadband subscribers, hardware-accelerated PPP over Ethernet and PPP over ATM, routed bridge encapsulation and 1483 routing. See page 1-47 for more information on the 10000 series.

Cisco 6400 Series

The Cisco 6400 is designed for use in high-availability environments such as service provider central offices, and corporate premises; and aggregates access media (DSL, cable, wireless, and dial) to serve as the intelligent equal access point, allowing multiple operating companies and service providers access to end users. It includes switch, router, and line card redundancy.

The Cisco 6400 is a high-performance service gateway that enables the delivery of network services, VPNs, and voice- and entertainment-driven traffic over any access media. ATM interfaces connect the Cisco 6400 to dial access servers, DSLAMs, and Cisco IP DSL Switches; ATM and packet interfaces connect to the network core.

Key Features

- Session scalability and modular design—The Cisco 6400 represents a quantum leap in session scalability, capable of scaling from 2000 subscribers in its entry level configuration to 96,000 subscribers in a full configuration.
- Routing and VPN scalability—Using the Cisco 6400, service providers can simultaneously route end-user traffic over secure, independent pathways exceeding 1000 different domains or end destinations, with an aggregate throughput of over 2.4 Gbps forwarding capacity for handling even the most bandwidth-intensive broadband traffic.

For More Information

See the 6400 series Web site: **http://www.cisco.com/go/6400**

ATM Multiservice WAN Switching

Cisco BPX 8600 Series—Advanced ATM Multiservice Switches

The Cisco BPX 8600 series is standards-based ATM switch with advanced IP and ATM capabilities. Designed to meet the demanding, high-traffic needs of a public service provider or large private enterprise, the BPX switch delivers high-performance ATM switching, multiservice adaptation and aggregation for all types of user traffic. Proven in the world's largest ATM and Frame Relay networks, the BPX 8600 enables service providers and large enterprises to meet skyrocketing network demands.

The Cisco BPX 8600 series switch offers up to 20 Gbps of high-throughput switching for multiple traffic types data, voice, and video and supports a wide range of interfaces, from Frame Relay to full broadband subscriber interfaces, up to 622 Mbps. You can offer multiple services for LAN, X.25, SNA, IP, Frame Relay, and ATM traffic from a single BPX platform. The Cisco BPX 8600 series supports multiprotocol label switching (MPLS) today, and this functionality can be easily added to any BPX switch already installed in the field.

For More Information

See the Cisco BPX Web site: **http://www.cisco.com/go/bpx**

Cisco MGX 8850 ATM Multiservice Switch

The Cisco MGX 8850 ATM Multiservice Switch enables delivery of a complete portfolio of service offerings while scaling from DS0 to OC-48c/STM-16 speeds. It enables service providers to be first to market with the new high-margin voice and data services while maintaining existing services.

The MGX 8850 universal chassis provides a unified ATM architecture that delivers a complete portfolio of differentiated services —from circuit emulation to IP VPNs—all with a single chassis, to enable service providers to easily add new services.

The Cisco MGX 8850 can function in three different modes of operation:

- PXM-1 configuration—Operates as a stand-alone device for narrowband services, or as an integrated edge concentrator for the Cisco BPX 8600 series or the Cisco MGX 8850 PXM-45
- PXM-1E configuration-Operates as a stand alone switch for low density narrowband services and included 1.2 Gbps switch card and PNNI routing
- PXM-45 configuration—Serves as a broadband edge switch and includes the 45 Gbps switch card and broadband ATM modules

Key Features

- Flexible ATM multiservice platform
- Highly scalable—from 1.2 to 45 Gbps of non-blocking throughput in single chassis
- Highest reliability, availability, and serviceability in the industry
- IP VPNs using Cisco IOS software-based Multiprotocol Label Switching (MPLS)
- Market-leading Frame Relay capabilities, with price-per-port leadership and advanced QoS
- High-density Point-to-Point protocol (PPP) for Internet access and aggregation
- Full-featured narrowband ATM for managed data, voice, and video services; high-density broadband ATM for wholesale ATM services
- Circuit Emulation for Private Line replacement
- Highly scalable packet voice gateway providing VoIP, VoATM(AAL1 & AAL2), ATM SVCs, Onboard MPLS

For More Information

See the Cisco MGX 8850 Web site: **http://www.cisco.com/go/mgx8850**

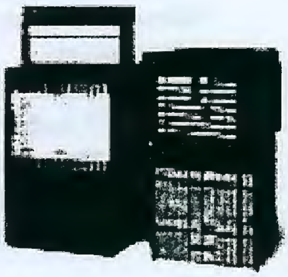
Cisco MGX 8830 ATM Multiservice Switch

The Cisco MGX 8830 Advanced ATM Multiservice Switch extends a full suite of narrowband interfaces and broadband trunking to remote sites with low density and high service mix requirements, using PNNI and MPLS for flexible network and services evolution. The Cisco MGX 8830, with a switching capacity of up to 1.2 Gbps, acts as a standalone switch, and offers a full range of service interfaces.

For More Information

See the Cisco MGX 8830 Series Web site: **http://www.cisco.com/go/mgx8830**

Cisco MGX 8200 Series



Cisco MGX 8230 Edge Concentrator

The Cisco MGX 8230 Edge Concentrator provides the most cost-effective gateway for narrowband services in space and power limited situations. It can acts as a stand-alone gateway or as an edge concentrator for the Cisco BPX 8600, Cisco MGX 8850 with PXM-45, and IGX 8400 series multiservice switches. The MGX 8230 offers a full range of narrowband service interfaces and a switching capacity up to 1.2 Gbps.

Cisco MGX 8250 Edge Concentrator

The Cisco MGX 8250 is a high-density edge concentrator designed for service providers needing flexibility for aggregation of IP, voice, Frame Relay, circuit emulation, and ATM services. An ATM narrowband edge concentrator, the MGX 8250 can serve as a stand-alone edge concentrator or as a feeder node for the Cisco BPX 8600 series and MGX 8850 switches. The MGX 8250 Edge Concentrator offers up to 1.2 Gbps of IP + ATM switching capacity.

For More Information

See the Cisco MGX 8200 Series Web site: **http://www.cisco.com/go/mgx8200**

Cisco IGX 8400 Series Multiservice WAN Switch

Efficient bandwidth utilization, intelligent QoS management features, and carrier-class reliability make the IGX 8400 series switch the ideal choice for meeting unique Wide-Area Networking (WAN) needs. This series provides the ATM backbone required to deliver data, voice, fax, and video services with guaranteed quality of service (QoS). The IGX 8400 series switch connects to public services for reduced leased-line costs by maximizing the use of these WAN links. Available with 8, 16, or 32 slots, the IGX 8400 series switches offers high flexibility to meet a wide range of Enterprise and Service Provider needs. Tight integration with the broad range of Cisco access products enables you to efficiently and cost-effectively run backbone-to-branch data, voice, fax, and video services between premises. By integrating IOS technology, the Cisco IGX 8400 series switch helps deliver a seamless migration path to technologies such as VoIP and MPLS.

For More Information

See the Cisco IGX 8400 Web site: **http://www.cisco.com/go/igx**

Cisco Long Reach Ethernet Solution

The Cisco Long-Reach Ethernet solution meets the demands of high bandwidth applications while leveraging existing copper wiring infrastructures. Catalyst® 2950 Long-Reach Ethernet (LRE) Series switches enable enterprise and service provider customers to extend intelligent Ethernet services over existing phone and legacy wiring, at distances of up to 5000 feet. Cisco is the only company with the breadth of technologies that allow customers to deliver intelligent network services across any combination of wired and wireless infrastructures.

The Cisco 2950 LRE solution includes the Cisco Catalyst® 2950 LRE switches, the Cisco 575 and 585 LRE Customer Premise Equipment (CPE) devices, and the Cisco LRE POTS Splitter. Each LRE link is terminated with either the Cisco 575 or 585 LRE CPEs, and a POTS splitter is required when POTS traffic coexists with the LRE link over the same line.

Catalyst 2950 LRE Series Intelligent Ethernet Switches

The Cisco Catalyst® 2950 LRE switches are fixed-configuration, stackable models that provide wire-speed LRE and Gigabit Ethernet connectivity for small and midsized networks. The Catalyst 2950 Series is an affordable product line that brings intelligent services, such as enhanced security, high availability and advanced quality of service (QoS), to the network edge-while maintaining the simplicity of traditional LAN switching. When a Catalyst 2950 LRE switch is combined with a Catalyst 3550 Series switch, the solution can enable IP routing from the edge to the core of the network. Embedded in Catalyst 2950 Series switches is the Cisco Cluster Management Suite (CMS) Software, which allows users to simultaneously configure and troubleshoot multiple Catalyst desktop switches using a standard Web browser. In addition to CMS, Cisco Catalyst 2950 LRE switches provide extensive management tools using Simple Network Management Protocol (SNMP) network management platforms such as CiscoWorks for Switched Internetworks.

The Cisco Catalyst 2950 LRE switches consist of the following devices-which are based upon the Enhanced Image (EI) Software for the Catalyst 2950 Series.

- Catalyst 2950ST-24-LRE-24 LRE ports + 2 10/100/1000BASE-T ports + 2 Small Form-Factor Pluggable (SFP) ports (two of the four uplinks active at one time)
- Catalyst 2950ST-8-LRE-8 LRE ports + 2 10/100/1000BASE-T ports + 2 SFP ports (two of the four uplinks active at one time)

The two built-in Gigabit Ethernet SFP ports support 1000BASE-SX and 1000BASE-LX modules. The dual SFP-based and copper Gigabit Ethernet implementation provides customers with tremendous deployment flexibility-allowing customers increased availability with the redundant uplinks. High levels of stack resiliency can also be implemented by deploying dual redundant Gigabit Ethernet uplinks and UplinkFast technologies for high-speed uplink and stack interconnection failover, and Per VLAN Spanning Tree Plus (PVST+) for uplink load balancing.

Cisco 575 and 585 LRE CPE Devices

Each LRE port is terminated in the room with either the Cisco 575 or 585 LRE Customer Premise Equipment (CPE) devices. These compact devices bridge LRE and Ethernet. The 575 CPE has one RJ-45 Ethernet connection and two RJ-11 connectors—one for the wall and one for a telephone. The 585 CPE has four RJ-45 switched Ethernet connections and two RJ-11 connectors and supports 802.1p QoS so that voice and video traffic are prioritized over normal data traffic. Both the Cisco 575 and 585 LRE CPE device can be mounted on or under a desk, or on a wall. They ship with a mount lock-in mechanism and clip-on Ethernet cable guard to discourage theft. It supports voice (Plain Old Telephone Service—POTS) traffic-including ISDN or digital phones-that coexists over the same LRE line by splitting LRE and POTS traffic at the CPE device.

Cisco LRE 48 POTS Splitter

The Cisco LRE 48 POTS Splitter is a high-density, low-cost device that is ideal for building deployments where the PBX system is on-site and POTS traffic must coexist over the same copper wiring as LRE traffic. Unlike "splitterless" building broadband network solutions, the Cisco LRE 48 POTS Splitter ships as a separate, compact form factor to ensure that POTS service is separate, and never compromised by LRE switch reconfigurations or downtime.

The Cisco LRE 48 POTS Splitter supports 48 ports in a 1RU form factor. Each splitter has six RJ-21 connectors-two each for connectivity to the patch panel, the LRE switch(es), and the on-site PBX system.

Key Features

- Performance—Delivers 2-15 Mbps symmetric over existing category 1/2/3 wiring at distances up to 5000 feet. Rate Selection feature automates the process of selecting a data rate for a line for ease of installation and increased robustness.
- Powerful Gigabit Ethernet uplink options—1000BaseT and SFP ports
- Superior control through intelligent services—advanced quality of service and security based on Layer 2 through Layer 4 parameters.
- Multicast support—Multicast VLAN Registration (MVR) and IGMP Snooping.
- Enhanced Cisco IOS Services
- Network Management—Cisco Switch Clustering technology and the advanced, Web-based Cisco Cluster Management Suite (CMS) software deliver easy-to-use configuration and ongoing monitoring and management of up to 16 switches. This software is embedded in the switches and delivers remote management of clustered switches and connected CPE devices through a single IP address

Competitive Products

- Paradyne Networks: BitStorm solution (Etherloop) and ReachDSL products
- Tut Systems: IntelliPOP VDSL
- Extreme Networks: Alpine chassis with FM-8Vi blade (Ethernet over VDSL)
- Huawei: Quidway s3026v

Specifications

Feature	Cisco 2950ST 24 LRE	Cisco 2950ST 8 LRE
Fixed Ports	24 Long-Reach Ethernet ports and four 10/100 Ethernet ports and 2 10/100/1000BASE-T ports + 2 Small Form-Factor Pluggable (SFP) ports (two of the four uplinks active at one time	12 Long-Reach Ethernet ports and four 10/100 Ethernet ports and 2 10/100/1000BASE-T ports + 2 Small Form-Factor Pluggable (SFP) ports (two of the four uplinks active at one time)
Backplane	8.8 Gbps	Same as Cisco 2950ST 24 LRE

Feature	Cisco 2950ST 24 LRE	Cisco 2950ST 8 LRE
Forwarding Rate	3.5 Mpps	3.2 Mpps
VLAN Maximum	250 port based VLANsor ISL/802.1Q trunks	Same as Cisco 2950ST 24 LRE
FEC	Yes	Same as Cisco 2950ST 24 LRE
802.1Q	Yes	Same as Cisco 2950ST 24 LRE
Multicast	IGMP Snooping	Same as Cisco 2950ST 24 LRE
QoS	802.1 p, 4 egress queues, WRR, Layer 3 and 4 services	Same as Cisco 2950ST 24 LRE
Management Capabilities	SNMP, Telnet, RMON, CWSI, CLI-based out-of-band, embedded Cisco Cluster Management Suite(CMS), Web-based interface	Same as Cisco 2950ST 24 LRE
Memory	84 MB (Flash); 32 MB (CPU DRAM)	Same as Cisco 2950ST 24 LRE
Embedded RMON	History, Events, Alarms, Statistics	Same as Cisco 2950ST 24 LRE
Dimensions (HxWxD)	1.75" (44.5 mm) x 17.5" (444.5 mm) x 9.7" (246.6 mm)	Same as Cisco 2950ST 24 LRE

Selected Part Numbers and Ordering Information[1]

Catalyst 2950 LRE Series Switches	
WS-C2950ST-24-LRE	Catalyst 2950 LRE switch: 24-port LRE + 2 10/100/1000BASE-T ports + 2 SFP ports
WS-C2950ST-8-LRE	Catalyst 2950 LRE switch: 8-port LRE + 2 10/100/1000BASE-T ports + 2 SFP ports
Cisco 575 and 585LRE CPE Device	
CISCO575-LRE	Cisco 575 LRE CPE device: 1-port Ethernet + 2RJ-11 connectors
CISCO575-LRE-6P	Cisco 575 LRE CPE device (6 pack): 1-port Ethernet +2 RJ-11 connectors
CISCO575-LRE-24P	Cisco 575 LRE CPE device (24 pack): 1-port Ethernet + 2RJ-11 connectors
CISCO585-LRE	Cisco 585 LRE CPE device: 4-port Ethernet + 2RJ-11 connectors
CISCO585-LRE-6P	Cisco 585 LRE CPE device (6 pack): 4-port Ethernet +2 RJ-11 connectors
CISCO585-LRE-24P	Cisco 585 LRE CPE device (24 pack): 4-port Ethernet + 2RJ-11 connectors
Cisco LRE 48 POTS Splitter	
PS-1M-LRE-48	Cisco LRE 48 POTS Splitter: 48 ports

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the LRE Web site: **http://www.cisco.com/go/lre**

Cisco Building Broadband Service Manager (BBSM) Version 5.2

Cisco Building Broadband Service Manager (BBSM) is an access gateway for public access networks that enables simple, plug-and-play access, end user self-provisioning of services, customizable portal and advertising platforms and Web-based management, reporting and configuration. In addition, multiple automated authentication and billing options are supported, including credit card, RADIUS, property management system and access code.

The Cisco BBSM platform manages Internet access services with no routine IT support, enabling property owners and service providers to offer services in remote and unattended locations. BBSM supports tiered service levels in order to deliver targeted customer offerings. For instance, a hotel can set-up daily network access for a series of meetings providing a variety of bandwidth/pricing options to capture lucrative meeting room revenue opportunities.

The Cisco BBSM has been designed for compatibility with Cisco access-layer LAN products to provide a complete solution that enables service providers or property owners to create, market and operate broadband access services in new vertical markets such as: Hospitality, Higher-Education, and Public Access

Cisco BBSM Hotspot Server Version 1.0

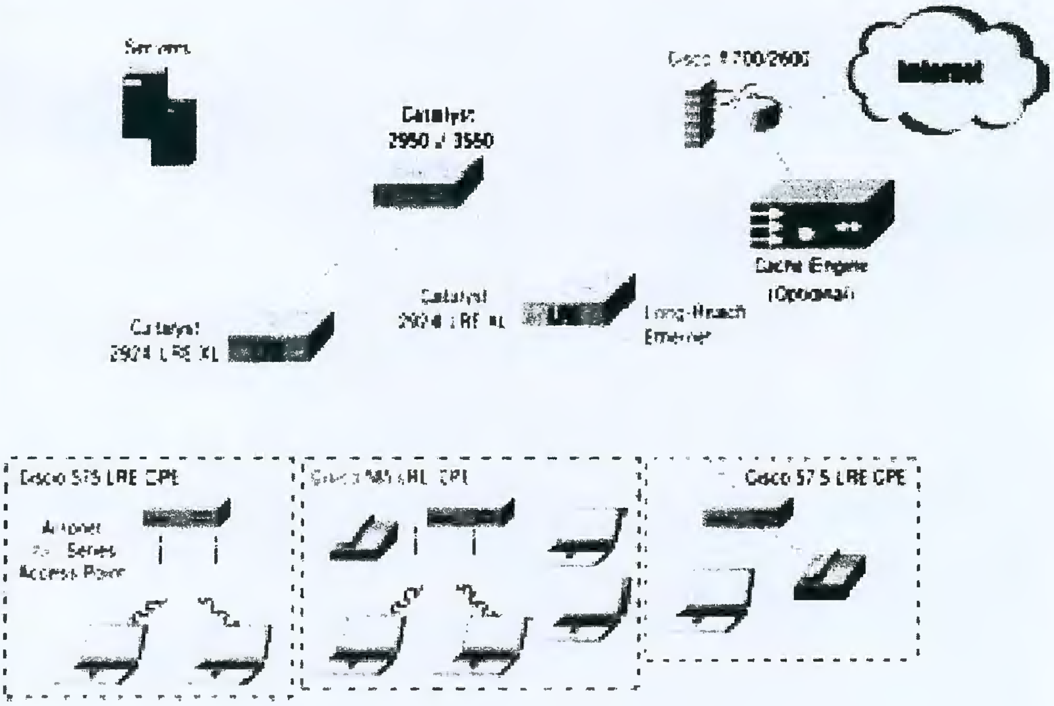
The Cisco Building Broadband Service Manager (BBSM) Hotspot server connects mobile users to broadband services anywhere, anytime. Cisco BBSM Hotspot is a cost effective access management gateway suited for small- to medium-sized public access locations, as well as for visitor access in larger enterprise locations. BBSM Hotspot enables simple plug-and-play connectivity, end user self-provisioning of services, and multiple authentication options.

BBSM Hotspot works with Cisco Local Area Network (LAN) products to provide a complete solution for secure wired and wireless Internet Access for visitors, guests and other temporary users. Use Cisco BBSM Hotspot to manage and operate broadband access services in public hotspots, small hotels, and public overlays on business networks.

For More Information

See the BBSM Web site: **http://www.cisco.com/go/bbsm**

Sample LRE Solution Overview—Broadband Internet Access for MxU



CHAPTER 8

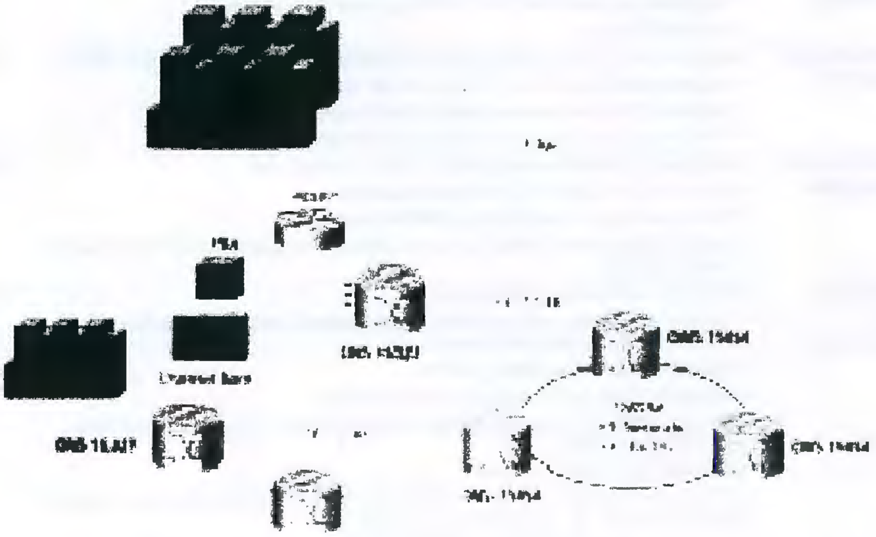
Optical Transport

Optical Transport Products at a Glance

Product	Features	Page
Cisco ONS 15200 Metro DWDM Series	Cisco ONS 15252 and ONS 15201 DWDM solutions • Supports a mixture of point-to-point,hubbed, and meshed traffic patterns (SDH/SONET, Gigabit Ethernet overa range of line rates up to 2.5 Gbit/s) • Modulararchitecture,capacitymay be addedchannel-by-channelin a highly cost-effective manner • High transmission efficiencyfor more channels, nodes and greater distances • Compact design	8-3
Cisco ONS 15302/15305 SDH Multiservice CPE & Aggregation Platforms	The Cisco ONS 15302/ONS 15305 Multiservice CPE and aggregation solutions are ultra-compact integrated systems that extend next-generation optical networks (access nodes or CPE): • Low Cost Access or CPE Platform • E1, E3, DS3, 10/100 BaseT Ethernet and GigE • STM-1 (15302) or STM-1/4/16 (15305)	8-3
Cisco ONS 15327 SONET Multiservice CPE & Aggregation Platform	Metro Edge Multiservice Provisioning Platform (MSPP) • Highly cost-efficient for delivering multiservices to the metro edge • Aggregates and switches TDM, 10/100/GigE, data and video services • Very small footprint	8-4
Cisco ONS 15454 SONET and ONS 15454 SDH Platforms	Industry-leading SONET Multi-service Provisioning Platform (MSPP) and SDH MSPP: • Aggregates DS1, DS3, STS-1, OC-3, OC-12, OC-48 • Supports OC-192 and mulitwavelength DWDM optics • Wide range of data interfaces, including 10/100/GigE, data and video	8-4
Cisco ONS 15501 Erbium Doped Fiber Amplifier	• Designed for Enterprise and Service Provider environments • Low-noise, gain flattened C-band optical amplifier • Complements the CiscoONS 155xx DWDM solution • Capable of extending 100GHz, 32-channel, 2.5Gbps / 10Gbps optical infrastructure over longer distances	8-5
Cisco ONS 15216 and 15501 Optical Transmission Families	Cisco ONS 15216 Metro DWDM Series • Supports 32 ITU-grid wavelengths at 100 GHz spacing and provides unprecedented transport flexibility with optical filtering • Optical Add/Drop Multiplexing (OADM) • Optical PerformanceMonitoring and Amplification • The ONS 15216 allows carriers to deliver more services per wavelength and more wavelengths per fiber Cisco ONS 15501 Optical Amplifier • Constant flat gain of 17 dB over the 1530nm to 1563nm band simplifies network design. • Metro optimized auto gaincontrol and variable gain • Low noise figure of <6.0 dB allows the use multiple amplifiers in cascade • Input power range of -29to 0 dBm	8-5
Cisco ONS 15530 Metro DWDM Aggregation Platform	Metro Optical DWDM Multiservice Aggregation Platform • Enables storage and data networking, transparent wavelength services, and legacy applications • ESCON Aggregation up to 40 channels on 1 wavelength • Scales from 2.5Gbps to 10Gbps • Supports wide range of protocolsover optical infrastructure • Highly resilient network with flexible topology design options	8-5

Product	Features	Page
Cisco ONS 15540 Extended Services Platform	Highly modular and scalable next-generation Dense Wave Division Multiplexing (DWDM) platform • Ideal for enterprises and service providers • Delivers the integration of data, storage and metro networking • Ultra-high bandwidth intelligent optical infrastructure • Supports any packet on any wavelength from any platform	8-6
Cisco ONS 15600 Multiservice Switching Platform (SONET/SDH)	The Cisco ONS 15600 MSSP is a true multiservice switch, providing carrier class reliability, availability, serviceability, operations, and management. • Combines the functionality of multiple metro systems including SONET/SDH multiplexers and digital cross-connect network elements • Scalable, easy-to-use platform supports all metro topologies	8-7
Cisco Transport Manager (CTM 4.x) (Network Management)	Carrier-class element management system • Ideal for service provider and enterprise networks • Supports Cisco ONS 15454/15327/15600 (SONET/SDH), 15540, 15530, 15501, 152xx, 1580X systems • Manages fault/performance/configuration/alarm/security/inventory/administrative tasks • Native Circuit/Equipment Provisioning for 15454/15327/15600 SONET/SDH product family • Northbound interfaces include SNMP, TL1 and CORBA • Integrates into OSS/BSS systems • Requires SUN/Solaris/UNIX server and Oracle database	8-8
Cisco 10720 Internet Router	Service provider-class metro access services router • Optimized building block for the next generation metro IP network • Equipped with 24 ports of Ethernet technology for customer access and dynamic packet transport (DPT) technology for metro optical connectivity • Powered by Cisco IOS software and the parallel express forwarding (PXF) architecture • Cost-effective, reliable platform supporting full suite of IP routing protocols • With DPT architecture, enables optimal fiber connectivity as well as features such as IP class of service, TLS, VoIP and VPN services See Chapter 1—Routers for more information on the Cisco 10720 Internet Router	1-49

Sample Metro Optical Transport Solution Overview—Delivering Multiservices to the Edge



Cisco ONS 15200 Optical Metro DWDM Series

The Cisco ONS 15252, 15201, and 15216 are part of the Cisco ONS 15200 Metro DWDM family, the first solution to deliver instant wavelengths to buildings, premises, or PoPs.

The ONS 15252 and 15201 may be used to realize many sub-network topologies and can handle a mixture of point-to-point, hubbed, and meshed traffic patterns. Capacity may be added channel-by-channel in a highly cost-effective manner. Since they feature broadband transponders, a wide range of traffic types may be handled (SONET/SDH, Gigabit Ethernet) over a range of line rates up to 2.5 Gbs. Channel protection options include unprotected, client-protected, and (optical channel) fiber protection. The ONS 15252 is a multi-channel unit and the ONS 15201 is a single channel unit node. Both have exceptionally small footprints and low power consumption.

The Cisco ONS 15216 supercharges wavelength services by supporting up to 32 ITU-grid wavelengths, and provides unprecedented transport flexibility with optical filtering, Optical Add/Drop Multiplexing (OADM), Optical Performance Monitoring and Amplification. It allows service providers to deliver more services per wavelength and more wavelengths per fiber.

The Cisco ONS 15216 optical filter solution enables service providers to deploy point-to-point, bus, and ring networks using the terminal filter multiplexing and demultiplexing and OADM. The Cisco ONS 15216 platform provides an open and flexible solution to combine wavelengths launched by the Cisco ONS 15454, ONS 15252, ONS 15201, and ONS 15540. The Cisco ONS 15216 supercharges wavelength services and extends Cisco's optical leadership to metro regional DWDM.

For More Information

See the ONS 15200 Series Web site: **http://www.cisco.com/go/ons15200**

Cisco ONS 15302/15305 SDH Multiservice CPE & Aggregation Platforms

The Cisco ONS 15302/ONS 15305 Multiservice CPE and Aggregation solutions are ultra-compact integrated systems that offer cost effective solutions with short ROI. These platforms provide native multiservice capabilities (i.e., TDM interfaces, multiplexing and Ethernet data interfaces). These products can be managed under Cisco Transport Manager (CTM), Cisco's unified optical network management system.

The ONS 15302 CPE platform provides the following TDM interfaces—STM-1 uplink (protected or unprotected STM-1 optical uplink, 1+1 MSP, future SNCP) and E1 customer interfaces (12 E1 ports). This product also provides native Ethernet customer access via 4-port 10/100BaseT module that supports full layer 2 capacity, bridging, VLANs, spanning tree, and priority management. An optional WAN module is available for point to multi-point applications.

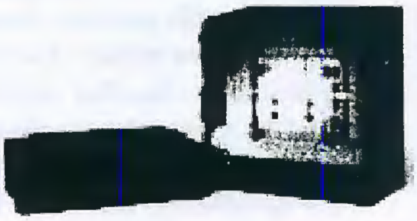
The ONS 15305 Aggregation platform provides the following TDM interfaces—protected or unprotected optical interfaces (8 port S-1.1 optical module, 2 port S-4.1 optical module, 1 port S-16.1 optical module, 1+1 MSP, SNCP, 2F MS-SPRing for STM-16) and electrical customer interfaces (8 and 63 port E1 modules and a 6-port

E3/DS3 module). This product also provides native Ethernet customer access via an 8-port 10/100BaseT module and a 2-port GigE module (supports full layer 2 capacity, bridging, VLANs, spanning tree, and priority management). An optional WAN module is available for point to multi-point applications.

For More Information

See the ONS 15302/ONS 15305 web site: **http://www.cisco.com/go/ons15300**

Cisco ONS 15454 and 15327 Multiservice Provisioning Platforms



The Cisco ONS 15454 and ONS 15327 Multi-service Provisioning Platforms (MSPP) are key building blocks in today's optical networks due to their unprecedented transport performance and economics. They offer supercharged transport capability by combining the best of traditional SONET TDM (time division multiplexing) and statistical multiplexing in single units.

The Cisco ONS 15454 aggregates traditional facilities such as DS1, DS3, STS-1, OC-3, OC-12, and OC-48 including multi-wavelength DWDM optics, but it also supports data interfaces for 10/100/GigE, data and video. This enables drastically improved efficiencies in the transport layer and breakthrough cost savings for initial and life cycle deployment. A single ONS 15454 shelf can support combinations of OC-3/c, OC-12/c, OC-48/c, and OC-192.

The new Cisco ONS 15454 SDH MSPP offers an international optical transport solution that combines the best of traditional SDH TDM and statistical multiplexing in a single platform. The Cisco ONS 15454 SDH MSP can aggregate traditional services such as E1, E3, DS3, STM-1, STM-4, STM-16 and STM-64 including multi-wavelength DWDM optics, but is also designed to support data interfaces such as Ethernet/IP.

The Cisco ONS 15327 combines industry-leading bandwidth capacity and service diversity in a very compact footprint, enabling service providers to achieve radical economics at the metro edge. Based on the same technology as the industry leading Cisco ONS 15454, the ONS 15327 supports high optical bandwidth and has the ability to drop a DS1 from an OC-48 stream. With comprehensive STS- and VT-level bandwidth management and integrated data switching, the Cisco ONS 15327 also serves as a digital cross-connect without the need for additional equipment. It aggregates and switches TDM, Ethernet, and ATM services, and can be managed using the Cisco Transport Manager element management system.

For More Information

See the ONS 15454 SONET Web site: **http://www.cisco.com/go/ons15454**

See the ONS 15454 SDH Web site: **http://www.cisco.com/go/15454sdh**

See the ONS 15327 Web site: **http://www.cisco.com/go/ons15327**

Cisco ONS 15501 Erbium Doped Fiber Amplifier

The Cisco ONS 15501 is a low-noise, gain-flattened C-band optical erbium doped fiber amplifier designed to extend the distance of today's metro high-bandwidth optical network beyond existing optical budget constraints. The Cisco ONS 15501 complements the Cisco ONS 155xx DWDM and Catalyst 6500 solutions, providing customers with the capability to extend their 2.5-Gbps or 10-Gbps optical infrastructures over greater distances. Packaged in a one-rack-unit (1RU) chassis, the Cisco ONS 15501 incorporates features such as 17-dB constant flat gain, automatic gain control, and low noise figure for excellent Optical Signal to Noise Ratio (OSNR) characteristics.

For More Information

See the Cisco ONS 15501 Web site: **http://www.cisco.com/go/ons15501**

Cisco ONS 15530

The Cisco ONS 15530 is a DWDM (dense wavelength division multiplexing) multiservice aggregation platform. The ONS 15530 can be used in applications such as storage networking, data networking, transparent wavelength services, and legacy SONET / SDH / ATM. These features make the ONS 15530 an excellent choice for building a scalable, ultra-high-bandwidth-ready, intelligent optical aggregation and transport infrastructure.

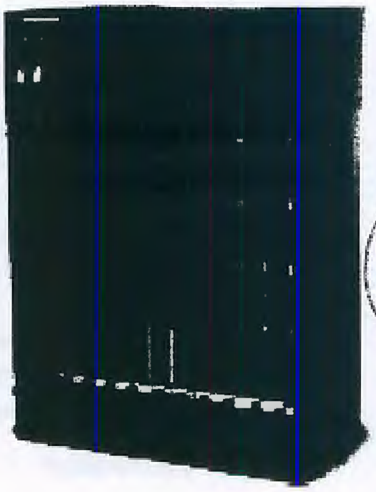
Key Features

- Aggregation—up to 40 ports of ESCON or 8 ports of Fibre Channel, FICON, or Gigabit Ethernet per wavelength, lowering total cost of ownership through bandwidth efficiency
- Scalability—up to 32 wavelengths ranging from 2.5Gbps to 10Gbps for network growth and design flexibility
- Multiservice Interfaces—protocol-independent transponders supporting data rates between 16Mbps to 2.5Gbps for protocols such as ESCON, FICON, Fibre Channel, 2G Fibre Channel, Gigabit Ethernet, SONET/SDH, Digital Video, and other protocols
- Cost-efficient point-to-point fiber trunk protection capability using the Protection Switch Module
- Complete Amplification Solution—Together with ONS 15501 EDFA optical amplifier, the VOA modules enables enterprises and service providers to further expand their optical DWDM networks over greater distances.
- Design Flexibility—can be used to deploy Point-to-point, Hub Ring, or Mesh Ring networks
- Network assurance—through high availability and resilient optical design
- IOS-based—easily integrates into existing Cisco networks

For More Information

See the Cisco ONS 15530 Web site: **http://www.cisco.com/go/ons15530**

Cisco ONS 15540 Extended Services Platform (ESPx)



The ONS 15540 Extended Services Platform with external cross connect capability (ESPx) is a highly modular, flexible, and scalable next generation dense wave division multiplexer (DWDM) platform that integrates data networking, storage area networking (SAN), time division multiplexing, (TDM) Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) technologies over an ultra high bandwidth, intelligent optical infrastructure that can support any packet, over any wavelength on any platform.

- Flexible Multi-Protocol Support—The Cisco ONS 15540 offers both variable rate transparent and fixed rate multi-protocol transponders that feature user selectable small form factor pluggables (SFPs) and support a variety of industry standard data rates between 16Mbps to 2.5Gbps as well as 10Gb Ethernet
- Scalable, flexible, and modular architecture in a high-density compact footprint—Provides superior operational support and network expansion on an as needed basis through its hot swappable modular lines cards, transponders, and optical multiplexers
- Simple Network Consolidation and Comprehensive Multi Service Support provided by the available ONS 15540 2.5GB and 10GbE transponders
- Optical, Service, and Application Level Performance Monitoring—provides industry-leading supports for service level agreements (SLAs)
- High Availability for mission critical networks—Provides 99.999% availability for demanding Managed Network Service Providers and enterprise business continuance applications, with hardware redundancy and automatic protection switching to protect against fiber cuts and equipment failures
- Multi-Service Integration—Transports ESCON, FICON, 1Gb/2GB Fibre Channel for Storage Area Networking (SAN), Fast and Gigabit Ethernet, and 10 Gb Ethernet for data networking, and SONET/SDH at OC-3/STM1, OC-12/STM4, and OC-48/STM12

Key Features:

- Compact modular design with external connectorization: External Direct Connect system from Line card to OADMs; Optional cross connect and fiber management system
- Transparent Tuneable Variable data rate Type 1 Transponders: 16Mbps to 622Mbps MM fiber support; 16Mbps to 2.5Gbp SM fiber support; 16 Tuneable transponders support 32 channels for reduced sparing costs; Multi-protocol support for Enterprise
- Tuneable Type 2 Transponders with Multi Protocol Small form Factor Pluggables (SFPs): Variable data rate support between 16Mbps to 2.5Gbps; 16 Tuneable transponders support 32 channels for reduced sparing costs; Multi-protocol SFP Support
- Standards based Management support for SNMP, Ciscoview and Cisco Transport Manager (CTM)
- Protection Switch Module provides highly cost effective solution for fiber trunk protection
- Standards based Optical architecture conforming to ITU G.692 100GHz channel spacing
- This system has been qualified by IBM for Geographically Dispersed Parallel Sysplex (GDPS), and by EMC for Symmetrix Synchronous support as tested in their E-LAB environment

For More Information

See the Cisco ONS 15500 Series Web site: **http://www.cisco.com/go/ons15500**

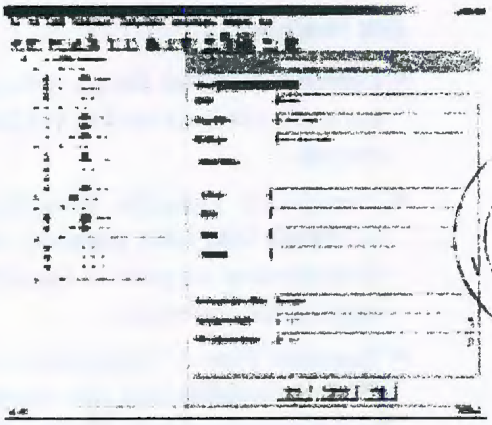
Cisco ONS 15600 Multiservice Switching Platform

The Cisco ONS 15600 provides unparalleled flexibility in designing next generation metro networks. Fully engineered and optimized for metro networks, the Cisco ONS 15600 MSSP simplifies and revolutionizes bandwidth management in the metro core by allowing service providers to seamlessly integrate their metro core and metro edge networks, while dramatically reducing initial turn up costs. Delivering scalability to 960 Gbps of traffic in a single rack, it complements the market-leading Cisco ONS 15454 Multiservice Provisioning Platform (MSPP) by leveraging its proven architecture and operating software. This allows service providers to dramatically simplify their metro networks and realize immediate cost, space and operational benefits. The Cisco ONS 15600 MSSP provides complete integration of metro core and edgenetworks for service provisioning and network management.

For More Information

See the ONS 15600 Series web site: **http://www.cisco.com/go/ons15600**

Cisco Transport Manager (CTM 4.x) (Element/Network Management)



7942
A.

Cisco Transport Manager is an integrated optical element management system for Cisco ONS 15000 series optical networking platforms. CTM manages configuration, fault isolation, performance, and security for Cisco optical network elements. With integrated support for SONET, SDH, DWDM and Ethernet, along with open interfaces to operations support systems (OSS), CTM delivers the full power of Cisco's wide range of advanced optical systems to today's network operators and enterprises.

CHAPTER 9

IOS Software & Network Management

Cisco IOS® Software & Network Management Products at a Glance

Product	Features	Page
CiscoWorks for Windows	An entry level suite of integrated network management tools for smaller networks: • Event management and topologymapping application • Includes Cisco's popular CiscoView Element Management Tool	9-2
Cisco IOS Software	Feature-rich network operating system supported on wide range of Cisco products • Provides a common IP fabric, functionality, and command-line interface (CLI) across network infrastructures • Enables a vast array of key routing, multiservice, traffic shaping, security/firewall, and traffic monitoring applications, and a broad variety of network connections	9-4
CiscoWorks Small Network Management Solution	Web-based network management solution designed for small to medium businesses (SMB) • Device auto-discovery using SNMP simplifies setup and reduces startup time • Standards-based, multi-vendor management • Event management and topologymapping application • Includes Cisco's popular CiscoView Element Management Tool	9-11
CiscoWorks Routed WAN Management Solution	A comprehensive set of applications formanaging the router elements of a multiservice Enterprise wide-area network. This bundle includesAccess Control List Manager, Internetwork Performance Monitor, Resource Manager Essentials, and CiscoView	9-13
CiscoWorks LAN Management Solution	Provides key applications neededto manage Cisco switch-based Enterpise campus networks. This bundle includes Campus Manager, Device Fault Manager, nGenius Real Time Monitor, Resource Manager Essentials, and CiscoView	9-14
CiscoWorks VPN/Security Management Solution	Combines general device management tools forconfiguring, monitoring, and troubleshooting enterprise networks with powerful security solutions for managing virtual private networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS). This bundle includes Management and Montoring Centers, Cisco IDS Host Sensor and Console, Cisco Secure Policy Manager, VPN Monitor, Resource Manager Essentials, and Cisco View	9-16
CiscoWorks Manager IP Telephony Environment Monitor	A suite of telephony management applicationsthat ensuresthe readiness and manageablity of convergednetworks supporting VoIP and IP telephonytraffic and applications. The bundle includes Voice Health Monitor, Default FaultManager, CiscoView, and DownloadableModules: IP Phone Information Utility, IP Phone Help Desk Utility, Fault History Manager	9-18
CiscoWorks Voice Manager for Voice Gateways	Enables the management and monitoring of devices used as gateways between analog voice equipment and the data network. • Enhanced capabilitiesto configure and provision voice ports • Create and modify dial plans on voice-enabled Cisco routers for voice over IP (VoIP), voice over Frame Relay (VoFR), and voice over ATM (VoATM) network deployments	9-19
CiscoWorks QoS Policy Manager (QPM)	Enables centralzed administrationand automated deployment of bandwidth reservation and prioritization policiesfor critical network applications • Differentiates services of Web applications, voice traffic, and business-critical applications	9-21
Cisco Ethernet Subscriber Solution Engine	A hardware-based managementsystem for metro access networks that use the Cisco ONT 1000 Gigabit Ethernet SeriesOptical Network Terminator. • Enables complete remote managementand troubleshooting of the customer demarcation point for Ethernet over fiber	9-22
CiscoWorks Hosting Solution Engine	A hardware-based contentmanagement solution for e-business operations in Cisco-powered data Centers. This product provides network infrastructure monitoring and Layer 4-7 hosted services configuration and activation.	9-24
CiscoWorks Wireless LAN Solution Engine	A hardware paced wireless LAN management solution that provides template-based configuation with user-defined groups to effectivelymanage a large number of access points and bridges • Monitors LEAP authenticationservers • Enhancessecurity management through mis-configuration detection on access points and bridges	9-23
Cisco Catalyst 6500 Series Network Analysis Modules 1 and 2	NAM is an integrated, netwok monitoring instrumentation and Web-browser based traffic analysis solution for the Catalyst 6500 based environments. It enable greater visibility into traffic at all layers of the networkby providing real time traffic analysis and troubleshooting capabilities.	9-25

Product	Features	Page
Cisco Secure User Registration Tool (URT)	Provides organizations with increased LAN security by actively identifies users within the network and createsuser registration policy bindingsthat help supportmobility and tracking: • Ensures that usersare associated with their authorized subnet/VLAN; Addresses the challenges associated with campususer mobility; Supports Web-based authentication for Windows, Macintosh, and Linux client platforms; Secure user accessto the VLAN with MAC address-based security option Option to allow multiple users connected toa hub accessto a VLAN served by single switch port See Chapter 5—VPN and Security for more information on Cisco Secure User Registration Tool	5-15
Cisco Secure Access Control Server (ACS) for Windows	Controls the authentication, authorizationand accounting (AAA) of users and administrators to network devices and services; Operates as a centralized Remote AccessDial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) server; Supports Lightweight Directory Access Protocol (LDAP) user authentication; Data replication and backup services; Flexible user and group policy controls; Support for Cisco 802.11x Catalyst Switch and Wireless solutions; Extensible Authenticaton Protocol (EAP)enhancementsto support Protected EAP (PEAP) for wireless LANs All administrative accessis encrypted with SSL See Chapter5—VPN and Securityfor more information on CiscoSecureAccessControl Server (ACS) for Windows	5-14

4940
A·

CiscoWorks for Windows

CiscoWorks for Windows is a powerful set of network management tools to easily manage your small to medium network or workgroup. It provides information such as dynamic status, statistics, and comprehensive configuration information for Cisco routers, switches, hubs, and access servers. Using the included WhatsUp Gold from Ipswitch, you can also monitor printer, workstations, servers and important non Cisco network services.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks for Windows	• A single solution for managing all resources attachedto a small multivendor network • A smaller solution, where centralizemanagementof configurationsof a software distribution is not needed • Low-cost network management • Needsto quickly understand basic network connectivity, accessindividual device configurations and statistics, and troubleshoot problems

Also available for small and medium size customers is the CiscoWorks Small Network Management Solution (Small NMS). Small SNMS includes all the features above and includes CiscoWorks Resource Manager Essentials (Essentials) which provides additional functionality that allows the customer to of build and maintain an up-to-date hardware and software inventory for up to 20 devices in a network.

Key Features

CiscoWorks for Windows provides the following features when used in conjunction with WhatsUp Gold from Ipswitch (included in the CiscoWorks for Windows package):

- Automatic discovery process for networked devices
- Management of network hardware, printers, servers, and workstations
- Customizable monitoring of services such as FTP and HTTP
- Access to extensive data on port status, bandwidth utilization, traffic statistics, protocol information, and other network performance statistics
- Flexible graphing capabilities for quickly recording and analyzing historical data that can be exported to files
- Management Information Base (MIB) compiler and browser for managing third-party SNMP devices
- Tools to simplify device configuration and management for Cisco routers, switches, and access servers
- Threshold management features that can be set for many performance variables to generate an alarm or event notification
- Flexible event notification, including voice, paging, and e-mail notification of user-defined events

CiscoWorks for Windows Components

CiscoWorks for Windows includes the following tools:

- WhatsUp Gold from Ipswitch, Inc.—Provides network discovery, mapping, monitoring, and alarm tracking
- CiscoView—Provides back- and front-panel displays; dynamic, color-coded graphical displays simplify device-status monitoring, device-specific component diagnostics, and application launching
- Threshold Manager—Enhances the ability to set thresholds on Cisco RMON-enabled devices, reducing management overhead and improving troubleshooting capabilities
- StackMaker—Allows users to combine multiple Cisco devices of specific types into a single stack and visually manage them in a single window
- Show Commands—Displays detailed router system and protocol information without requiring the user to remember complex Cisco IOS Software command-line languages or syntax

Specifications

Feature	CiscoWorks for Windows
Hardware Requirements	266 MHz Pentium-based IBM PC or compatible computer 128-MB RAM total 1 GB free hard drive space
Software Requirements	Windows 98, Windows NT 4.0, or Windows 2000 Netscape 461, 4.7, 4.76 or Internet Explorer 5.0, 5.1, 5.5

Selected Part Numbers and Ordering Information

CiscoWorks for Windows	
CWW-6.1-WIN	CiscoWorks for Windows 6.1
CWW-6.1-WIN-UP	Upgrade to CWW 6.1 for Windows from CWW 5.0
CWW-6.1-WIN-MR	Maintenance Release: Requires existing CWW 6.0 - June 02

For More Information

See the CiscoWorks for Windows Web site: **http://www.cisco.com/go/cwwin**

7938
3

Cisco IOS® Software

Cisco's IOS Software is a feature-rich network operating system that provides network intelligence for the majority of today's Internet and for most of the world's business-critical networking applications.

Supporting Cisco's extensive range of platforms, Cisco IOS Software provides a common IP fabric, functionality and command-line interface (CLI) across network infrastructures. Cisco IOS Software enables a vast array of key routing functions, multi-service capabilities, traffic shaping, connections, security/firewall protection, traffic monitoring, and highly flexible network and product configuration.

Below is an abbreviated list of key capabilities, intelligent network technologies, and architectures enabled by Cisco IOS Software:

- Quality of Service (QoS)
- Converged data, voice, and video over IP
- IP/ATM/Frame Relay network connectivity and scalability features
- Security/firewall/IPSec/access lists
- Traffic monitoring and NetFlow based monitoring, accounting, and billing
- Wide range of routing protocols (including MPLS)
- IPv6
- Multicast

Quality of Service (QoS)

The promise of networking is sharing networked resources among many users and applications for greater productivity and competitive advantage. Cisco IOS quality of services (QoS) capabilities enable complex networks to control and predictably service a variety of applications. Every network needs QoS for optimum efficiency, whether it is for a small business, large enterprise, or a service provider.

QoS expedites the handling of mission-critical applications, while sharing network resources with non-critical applications. QoS also ensures available bandwidth and minimum delays required by time-sensitive multimedia and voice applications. It also gives network managers control over network applications, improves cost-efficiency of WAN connections, and enables advanced differentiated services. QoS technologies are elemental building blocks for other Cisco IOS enabling services—particularly for converged data and voice networks (LAN/WAN + telephony), video conferencing over IP, and IBM networking, and for future business applications in campus, WAN, and service provider networks.

Key QoS Capabilities:

Committed Access Rate (CAR)	Performs two QoS functions • Bandwidth management throughrate limiting, which allows you to control the maximum rate fortraffic sent or received onan interface • Packet classificationthrough IP precedence and QoS group setting, which allows you to partitionyour network into multiple priority levels or classes of service (CoS)
Differentiated Services (DiffServ)	QoS architecture that divides traffic into a small number of classes and provides QoS to large aggregates of traffic bytreating sometraffic better than the est (faster handling, more bandwidth on average, lower loss rate on average). This is a statistical preference, not a hardand fast guarantee.
Expedited Forwarding (EF)	Per-Hop Behavior (PHB) in the DiffServ standard, used to create avirtual leased line service.

Integrated Services (IntServ)	A QoS architecture in which each network element is required to identify the coordinated set of QoS control capabilities it provides in terms of the function it performs, the information it requires, and the information it expots.
Random Early Detection (RED)	Monitors traffic levels on very large networks to prevent congestion and guarantee priority traffic delivery.
Resource Reservation Protocol (RSVP)	A protocol that supports the reservation of resources across an IP network.
Weighted Fair Queueing (WFQ)	Adds new levels of control to previous queuing methods
Weighted Random Early Detection (WRED)	Combines the capablities of the random early detection (RED) algorithm with IP precedence or the differentiated services code point (DSCP). This combination provides for preferential traffic handling for higher-priority packets.

Key QoS Categories

Classification	• Committed Access Rate (CAR) • Policy Based Routing (PBR) • QoS Policy Propagation Though BGP
Congestion Management	• First in First Out (FIFO) • Priority Queueing (PQ) • Custom Queueing (CQ) • Weighted Fair Queueing (WFQ) • Weighted Random Early Detection (WRED)
Policy and Shaping	• Committed Access Rate (CAR) • Generic Traffic Shaping (GTS) • Frame Relay Traffic Shaping (FRTS)
Link Efficiency Mechanisms	• Compressed Real Time Protocol (CRTP) • Link Fragmentation and Interleaving (LFI) • Data Compression

Converged LAN/WAN and Telephony Networks

A broad range of Cisco products support standards-based voice over packet implementations, including H.323-based Voice over IP (VoIP). These products enable highly efficient, converged IP-based telephony in today's enterprise and service provider networks, thereby eliminating the need for legacy telephone equipment and overlay networks (including PBXs and central office circuit switched network equipment). Furthermore, a single IT organization can now support campus and enterprise requirements—regardless if for data, voice, or video requirements.

In addition, Cisco voice over packet technologies enable businesses and service providers to avoid long distance telephone charges by leveraging their existing data networks, instead of paying for dedicated voice connections and circuits.

Cisco Connectivity and Scalability Solutions

A wide range of access solutions are enabled via Cisco IOS Software including:

- Virtual Private Networking; DSL; Dial Access (including ISDN, modem, fax, voice)
- Frame Relay, X.25
- ATM; VoIP, VoFR, VoATM
- SONET, OC-x/STM-x, Packet-over-SONET
- Broadband Services Aggregation (includes large-scale PPPoE, PPPoA, L2TP tunneling)
- Cable Access Solutions

Security

Cisco's powerful suite of Cisco IOS Software-embedded security and firewall technologies includes:

Digital Signature Standard (DSS) and digital certification	Positively authenticates users or devices
Network Address Translation (NAT) and Port Address Translation (PAT)	Hides private topology and IP addresses from an external network
IPSec	Enables secure communications of data over public networks

Time-based Access Control Lists (ACLs)	Implements access lists based on time of day
Password Authentication Protocol (PAP)	Allows a remote node to establish its identity using a two-way handshake
Terminal Access Controller Access Control System Plus (TACACS+) and Remote Access Dial-in User Service (RADIUS)	Gives complete network access security for dial-in connections, for enterprise and service provider applications
Challenge Handshake Authentication Protocol (CHAP)	Allows a remote node to establish its identity using a three-way handshake
Calling Line Identification (CLID)	Uses calling line identification to compare the telephone number of a calling device against a list of known callers
Access Lists	Checks the source address of packets (standard access lists) and checks the source and destination addresses and other parameters (extended access lists)
Context-Based Access Control (CBAC)	Provides secure, application-based stateful filtering for the most popular protocols and a wide variety of advanced applications; available in the Cisco IOS Firewall feature set

Cisco IOS NetFlow

NetFlow technology provides the metering base for a key set of applications including network traffic accounting, usage-based network billing, network planning, network monitoring, outbound marketing, and data mining capabilities for both service provider and enterprise customers. Cisco provides a set of NetFlow applications to collect exported NetFlow data, to perform data volume reduction, and to post-process and display data. Cisco is currently working with a number of partners to provide customers with comprehensive solutions for NetFlow-based billing, planning, and monitoring. NetFlow also provides the measurement base for Cisco's new Internet Quality of Service (QoS) initiatives. NetFlow captures the traffic classification or precedence associated with each flow, enabling differentiated charging based on Quality of Service.

Furthermore, the combination of NetFlow data along with Cisco IOS Software-based routing information can prove key to developing effective security policies and preventive measures for Denial of Service (DoS).

Cisco IOS Routing Services

Cisco IOS Software has long been recognized for its rich support of multiple protocols including IP, Novell IPX, SNA, AppleTalk, DECnet, OSI, and Banyan VINES

IP Routing Protocols

Cisco IOS Software offers the industry's widest variety of enterprise and service provider-class routing protocols, including On Demand Routing (ODR), Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), IP Multicast, Integrated IS-IS, Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), and MPLS

Multi Protocol Label Switching (MPLS)

Cisco IOS MPLS fuses intelligent routing capabilities with the performance of switching. It provides significant benefits to networks with pure IP architectures and those with IP and ATM or a mix of other Layer 2 technologies. MPLS technology is key to implementing scalable Virtual Private Networks (VPNs) and end-to-end QoS, enabling efficient utilization of existing networks to meet growth needs and to rapidly correct link fault and node failure. This technology also helps deliver highly scalable, differentiated IP services with simpler configuration, management, and provisioning for both Internet service providers and end-user customers.

Common MPLS Applications Available with Cisco IOS Software

- Traffic engineering is enabled through MPLS mechanisms that allow traffic to be directed through a specific path, which may not necessarily be the least-expensive path. Network managers can implement policies to ensure optimal traffic distribution and improve overall network utilization
- Guaranteed bandwidth is a value-added enhancement to traditional traffic-engineering mechanisms. MPLS lets service providers deliver guaranteed pipes and bandwidth allocations. Guaranteed bandwidth also allows bookkeeping of quality-of-service (QoS) resources to traffic engineer both premium and best-effort traffic such as voice and data
- Fast reroute (FRR) allows extremely quick recovery if a node or link fails. Such fast recovery prevents end-user applications from timing out and also prevents loss of data
- MPLS VPNs greatly simplify service deployment compared to traditional IP VPNs. As the number of routes and customers increases, MPLS VPNs easily scale, while providing the same level of privacy as Layer 2 technologies. In addition, they can transport non-unique IP addresses across a public domain
- MPLS class-of-service (CoS) capability ensures that important traffic is given the appropriate priority over the network and that latency requirements are met. IP QoS mechanisms can be seamlessly implemented in an MPLS environment

MPLS Mechanisms

Cisco IOS MPLS delivers both traffic engineering (TE) and VPN solutions built on the following mechanisms:

- Cisco AutoBandwidth Allocator: Automatically increases or decreases MPLS TE tunnel bandwidth based on measured traffic load
- Constraint-based Routing Label Distribution Protocol (CR-LDP): A signaling mechanism used to support TE across a MPLS backbone
- Fast Reroute (FRR): Enables quick recovery in case of link failures, which prevents end-user applications from timing out and also prevents loss of data
- Label Distribution Protocol (LDP): Provides communication between edge and core devices. It assigns labels in edge and core devices to establish Label Switched Paths (LSPs) in conjunction with routing protocols such as OSPF, IS-IS, EIGRP, or BGP
- Transmission Control Protocol (TCP): Connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. Part of the TCP/IP protocol stack

For More Information

See the Cisco IOS MPLS Web site: **http://www.cisco.com/go/mpls**

IP Multicast and Multicast Solutions

IP Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast technologies include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

Multicast technology is key to preventing severe network slowdown and Cisco IOS Multicast is the gateway to Internet broadcasting applications. Internet service providers (ISPs) and content providers use Cisco IOS multicast solutions successfully to host events such as live concerts, radio shows, and football games.

Another application of multicast technologies relates to replacing dedicated point-to-point telephone/voice circuits and specialized bridging and mixing multi-user audio conferencing telephone equipment for “always-on” service (referred to in some industries as “Hoot & Holler” systems). This ability eliminates the need for dedicated, costly, overlay voice networks and point-to-point telephone company circuits, and allows the same capabilities to be implemented over a converged IP network without requiring users to dial in.

Multicast Solutions

Cisco IOS Multicast solutions are classified as Multicast-Lite, Core Multicast, and Enhanced Multicast, and are the building blocks for Internet broadcast. Customers can start with Multicast-Lite, then add more sophisticated interactive communication capabilities, as needed.

- Multicast-Lite provides for one-to-many broadcast capability with no back channel. This solution is eminently suitable for content distribution and broadcasting over the Internet. It does not require setting up of source discovery across domains and autonomous systems. Multicast Lite includes Protocol Independent Multicast version 2 (PIMv2), Internet Group Management Protocol (IGMPv1/v2/v3) or Universal Resource Locator Rendezvous Directory (URD).
- Core Multicast provides interactive, reliable campus multicast for interactive distance learning, corporate videoconferencing, inventory updates, software distribution, and content distribution. Core Multicast includes PIM, IGMP, Cisco Group Management Protocol (CGMP), and now Pragmatic General Multicast (PGM).
- Enhanced Multicast provides interactive Internet Multicast across domains for network gaming, inter-company conferencing, Internet software distribution, and extranet content distribution. Enhanced Multicast includes Multicast Border Gateway Protocol (MBGP) and Multicast Source Discovery Protocol (MSDP) in addition to all the protocols supported in Core Multicast.

Multicast is available across all Cisco IOS Software-based platforms, including Cisco routers and Catalyst family switches. Multicast-supported routing platforms include the following: Cisco 1600, 2500, 2600/2600XM, 3600, 3700, 3800, 7200, 7500, and 12000 series; it also is available on Catalyst 6000 and 8500 platforms.

Multicast Features

Cisco has the greatest depth of experience with IP Multicast in the industry, and offers multicast features such as:

Bi-dir PIM	An extension to the PIM suite of pdocols that implements shared sparse trees with bi-directional flowof data.
Cisco Group Management Protocol (CGMP)	Cisco-develbped protocol that allows Layer 2 switches to leverage IGMP information on Cisco routers tomake Layer 2 forwarding decisions.
Internet Group Management Protocol v2 (IGMP)	Used by IP routers and their immediately connectedhosts to communicate multicast group membership states: • Query: IGMP messages originating from the router(s) to elict multicast group membership information from its connected hosts • Report: IGMP messages originatingfrom the hosts that are joining, maintaining or leaving their membership in a multicast group
Internet Group Management Protocol v3 (IGMP)	Version 3 of IGMP adds support for "source filtering," that is, the ability for a system to report interest in receiving packetsonly from specific source addresses, or from all but specific source addresses, sent to a particular multicast address.
IGMP Snooping	Requires the LAN switch to examine, or "snoop," some Layer 3 information in the IGMP packet sent from the host to the router. When the switch hears an IGMP Report from a host for a particular multicast group,the switch adds the host's port number to theassociated multicast table entry. When it hears an IGMP Leave Group message from a host, it removes the host's port from the table entry
Inter domain Multicast	Supportsinter-domain routing and source discovery across the Internet or across multiple domains comprising an enteprise
Intra domain Multicast	Supports mukicast applicationswithin an enterpise campus
Multicast Source Discovery Protocol (MSDP)	A mechanism to connect multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) (RPs) in different domains.
Multicast Routing Monitor (MRM)	A managementdiagnostictool that provides network fault detection and isolation in a large multicast routing infrastructure
Multi-protocol Extensions for Border Gateway Protocol (MBGP)	Also known as BGP+, MBGP adds capabilties to BGP to enable mukicast routing policy throughoutthe Internet and to connect multicast topologieswithin and between BGP autonomous systems.
Pragmatic General Multicast (PGM)	A reliable multicast transport protocol for applications that require ordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers. PGM guaranteesthat a receiver in a multicast group either receives all data packets from transmissions and retransmissions, or can detect unrecoverable data packetloss.
Protocol Independent Multicast (PIM)	A multicast routing architecture that enables IP multicast routing on existing IP networks: • SM = Spare Mode (RFC 2362): Relies upon an explicitly joining method beforeattempting to send multicast data to receivers of a multicast group. • DM = Dense Mode (Internet Draft Spec): Actively attempts to send multicast data to all potential receivers (flooding) and relies upon their self-pruning (removal from group) to achieve desired distribution.
Unidirectional Link Routing (UDLR) Protocol	A routing protocol that provides a way to forward multicast packets over a physical unidirectional interface (such asa satellite link of high bandwidth) to stub networks that have a back channel
URL Rendezvous Directory (URD)	Directly provides the network with information about the specificsource of a content stream. It enablesthe network to quickly establish the most direct distribution path from the source to the receiver, thus significantly reducing the time and effort required in receiving the streaming media. URD allows an applicationto identify the source of the contentstream through a web page link or web directly.

For More Information

See the Multicast Web site: **http://www.cisco.com/go/multicast**

IPv6

Internet Protocol version 6 (IPv6), most notably offers expanded IP addresses to accommodate the proliferation of Internet devices such as personal computers, personal digital assistants, wireless devices, and new Internet appliances—and the expansion of Internet access, particularly "always-on" connections throughout the world. IPv6 also provides integrated auto-configuration for "plug-and-play" capabilities, enhanced mobility and end-to-end security.

Incorporating IPv6 into Cisco IOS Software further enables growth of the Internet and expansion into new applications and capabilities, while maintaining compatibility with existing Internet services. Cisco's IPv6 solution was first made available in Cisco IOS Software Release 12.2(1)T. Platforms supported include: Cisco 800, 1700, 2500, 2600/2600XM, 3600, 7100, 7200, and 7500 Series Routers, and Cisco AS5300 and AS5400 Universal Access Servers.

For more information

See the Cisco IOS IPv6 Web site: **http://www.cisco.com/go/ipv6**

Cisco IOS Software Release Process

There are three categories of Cisco IOS Software releases: Early Deployment, Major, and General Deployment (GD) releases.

- Early Deployment releases (i.e. T, S, X, E release families)—Provide advanced networking technologies to customers for delivery of leading-edge Internet applications. These offer new software capabilities, new platforms, and interface extensions. Customers for whom receiving a new feature is critical to their competitive advantage will benefit from these releases
- Major releases (i.e. Release 12.2)—Consolidate features, platform support, and functionality from early deployment releases, and emphasize stability. Regular maintenance releases do not introduce new functionality or platform support, but provide continuous improvement and greater quality, leading to general deployment
- General Deployment certification (i.e. Release 12.0) Releases—Have had extensive market exposure in a wide range of network environments and are qualified through extensive metrics that analyze stability, software defect trends, and customer satisfaction surveys. Used for major, business-critical applications

At some point, GD releases are replaced by newer releases with the latest networking technologies. A release retirement process has been established with three principal milestones: End of Sales (EOS), End of Engineering (EOE), and End of Life (EOL).

For More Information on Cisco IOS Software

See the Cisco IOS Software Web site: **http://www.cisco.com/go/ios**

Cisco Network Management Overview

Cisco is transforming traditional network management by focusing on the strengths of Internet-based architectures for greater accessibility and simplification of network management tools, tasks, and processes. Cisco's network management strategy calls for a Web-based model with the following characteristics:

- Simplification of tools, tasks, and processes
- Web-level integration with NMS platforms and general management products
- Capable of providing end-to-end solutions for managing routers, switches, and access servers
- Creation of a management intranet by integrating discovered device knowledge with CCO and third-party application knowledge

Cisco Network Management Products

The CiscoWorks product line offers a set of solutions designed to manage the enterprise network. These solutions focus on key areas in the network such as; optimization of the wide area network (WAN), administering switch-based local area networks (LAN), securing remote and local virtual private networks, and measuring service level agreements within all types of networks. The expanding CiscoWorks product line offers the flexibility to deploy end-to-end network management when and where it is needed.

CiscoWorks Small Network Management Solution

CiscoWorks SNMS is a new network management solution aimed at small to medium businesses (SMB), with 20 or fewer switches, routers, hubs and access servers. CiscoWorks SNMS can also monitor non-Cisco IT assets such as servers, applications, services and printers. CiscoWorks SNMS is an ideal solution for companies that need centralized network management to help optimize performance and maximize network productivity.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Small Network Management Solution	• Simple integrated installation,autodiscovery and automated import of devices using SNMP • Standards-based multi vendor management • Reduce the time and complexity of keeping the networks' configuration, software version and connectivity optimized

Also available for small and medium size customers is the CiscoWorks for Windows (CWW). CWW includes all the features above except for CiscoWorks Resource Manager Essentials (Essentials) which provides additional functionality that allows the customer to of build and maintain an up-to-date hardware and software inventory for up to 20 devices in a network.

Key Features

- Monitors and reports on hardware, configuration, and inventory changes
- Provides a wizard-based approach for managing and deploys configuration changes and software image updates to multiple Cisco devices
- Allows configuration changes to be performed against multiple switches or routers in the network
- Provides software update analysis reports showing prerequisites and impacts of proposed updates
- Provides a comprehensive audit of network changes, showing who changed what, when, and how
- Summarizes syslog events by severity or user criteria for switches, routers, and Cisco IOS and PIX firewalls
- Discovery and mapping wizard displays customizable vector-based graphics and hierarchical maps of networked devices

CiscoWorks Small Network Management Solution Components

CiscoWorks Small Network Management Solution includes the following tools:

- CiscoView 5.3—Provides graphical back and front panel views of Cisco devices; dynamic, color-coded graphical displays to simplify device-status monitoring, device-specific component diagnostics, device configuration, and application launching
- WhatsUp Gold 7.0 from Ipswitch, Inc.—Provides network discovery, mapping, monitoring, and alarm tracking
- Resource Manager Essentials 3.3.2—Resource Manager Essentials (RME) provides tools for building and managing network inventory, deploying configuration and software image changes, archiving configurations, and providing an audit trail of network changes

Important: RME has a device limit of 20 or fewer Cisco devices.

Specifications

Feature	CiscoWorks Small Network Management Solution
Hardware Requirements	2 Pentium III or better-based IBM PC or compatible computer, 256 MB RAM total, 4 GB free hard drive space
Software Requirements	Windows 2000 with SP1 or 2 (Professional or Sever), Netscape 4.77, 4.78 or Internet Explorer 5.5 with Service Pack 1

Selected Part Numbers and Ordering Information

CiscoWorks Small Network Management Solution	
CWSNM-1.0-WIN	Small Network Management Solution 1.0 for Windows; includes WhatsUp Gold 7.0, Resource Manager Essentials 3.3.2 (20 Cisco Device restriction), CiscoView 5.3

For More Information

See the CiscoWorks Small Network Management Solution Web Site:
http://www.cisco.com/go/wrsnms

CiscoWorks Routed WAN Management Solution

The RWAN solution addresses the needs of managing WANs by improving the accuracy, efficiency, and effectiveness of your network administrators and operations staff while increasing the overall availability of your network through proactive planning, deployment, and troubleshooting tools. The CiscoWorks Routed WAN Management Solution provides increased visibility into network behavior, assists in quickly troubleshooting performance bottlenecks, and provides comprehensive tools to easily administer new software and configuration changes for optimizing bandwidth and utilization across expensive and critical links in the network.

When to Sell

Sell This Product	When a Customer Needs These Features
Routed WAN Management Solution	• Optimize router performance by automatically streamlining access control lists, and applying policy-based changes via templates • Understand the responsiveness of WAN connections to determine where bottlenecks are; provides real-time analysis of end-to-end hop delays • Increase network performance by monitoring traffic of protocols, applications, and interface characteristics • A watchdog system to monitor WAN characteristics • An accurate inventory baseline; including memory, slots, software versions, and boot ROMs needed to make decisions • Automate the process of updating device software and configuration • Graphically displays a devices operational status with tools to monitor its activity or change its configurations • Support for secure browser communications and downloads from CiscoView, RME and ACLM via Secure Socket Layer(SSL) or Secure Shell (SSH) protocol

Key Features

- Access Control List Manager—Provides a wizard and policy template-based approach to simplifying the setup, management, and optimization of Cisco IOS Software-based IP and Internetwork Packet Exchange (IPX) traffic filtering and device access control
- Internetwork Performance Monitor—Used to diagnose latency, identify network bottlenecks, and analyze response times
- Resource Manager Essentials—Provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis
- CiscoView—Provides back- and front-panel displays; dynamic, color-coded graphical displays simplify device-status monitoring, device-specific component diagnostics, and application launching
- CiscoWorks Server—Provides the common management desktop services and security across the CiscoWorks family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications
- Support for secure browser communications with CiscoView and RME sessions via Secure Socket Layer (SSL) and Secure Shell (SSH) protocol

Specifications

Feature	Routed WAN Management Solution Requirements
Server	Sun UltraSPARCIII (Sun Blade1000 Workstation or Sun Fire 280R Workgroup Server) IBM PC compatible with 550-MHz or higher Pentium III processor running (Dual processor system required for hosting multiple management solutions) Microsoft Windows2000 Server or Professional Edition with Service Pack 2, Solaris 2.8
Client	IBM PC-compatible computer with 300-MHz or higher Pentium processor, Sun Ultra 10, HP9000 Series, IBM RS/6000 Windows NT 4 (Workstation and Server) with Service Pack 6a, Windows 98, 2000 Professional and Server with Service Pack 2; Solaris 2.7, 2.8; HP-UX 11.0; AIX 4.3.3 IBM PC-compatible computer with 300-MHz or higher Pentium processor, Sun Ultra 10, HP9000 Series, IBM RS/6000
Supported Devices	Most Cisco IOS Software routers, access servers, hubs, and switches
Supported Cisco IOS Software Versions	Generally supports Cisco IOS Software Versions 10.3 and above; Catalyst Supervisor code 2.1 and above Note: Some CiscoWorks applications require specific versions of IOS and CAT these releases in order to operate; please see the specific application documentation and releas notes for more information.

Selected Part Numbers and Ordering Information[1]

Cisco Routed WAN Management Solution

CWRW-1.2-K9	Routed WAN Management Solution 12 for Windows and Solaris platforms; includes Access Control List Manager 1.4, Internetwork Performance Monitor 2.4, Resource Manager Essentials 3.4, CD One 5th Edition (IncludesCiscoView 5.4)
CWRW-1.2-P1-K9	Cross Bundle Discount RWAN 1.2 for Windows and Solaris platforms; available to customers who have previously purchased LMS 1.X or LMS 2.X and want to add RWAN
CWRW-1.2-MR-K9	Maintenance kit for customers that purchased RWAN 1.X and now want new device support and code upgrades; kit includes support for Windows and Solaris platforms; includes updates to all components

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Routed WAN Management Solution Web site: **http://www.cisco.com/go/rwan**

CiscoWorks LAN Management Solution

The CiscoWorks LAN Management Solution consists of operationally focused tools. These tools include fault management, scalable topology views, sophisticated configuration, Layer 2/3 path analysis, voice-supported path trace, traffic monitoring, end-station tracking workflow application servers management, and device troubleshooting capabilities. CiscoWorks LMS combines applications and tools for configuring, monitoring, and troubleshooting the campus network.

When to Sell

Sell This Product	When a Customer Needs These Features
LAN Management Solution	• A set of tools for managing Cisco's award winning Catalyst switches • Time saving user tracking and path trace analysis tools with support of IP phones • Automated process of inventorying network devices, updating device software, and managing configuration to reduce the time and errors involved in network updates • Browser-accessible, graphical tool for configuring and monitoring Cisco device components and operational status • VLAN, ATM, or LANE service management tools • RMON traffic monitoring and analysis capability • Active fault monitoring of Cisco devices

Key Features

- Campus Manager—Web-based applications designed for managing Layer 2 device and connectivity discovery, workflow application server discovery and management, detailed topology views, virtual LAN/LAN Emulation (VLAN/LANE) and ATM configuration, end-station tracking, Layer2/3 path analysis tools, and IP phone user and path information
- Device Fault Manager—Provides real-time fault analysis for Cisco devices, automatically includes Cisco devices into its monitoring environment and applies a Cisco "Best Practices" fault rule to each device
- nGenius Real Time Monitor—Web-enabled multiuser traffic management tool set that provides access to network-wide, real-time RMON information for monitoring, troubleshooting, and maintaining network availability
- Resource Manager Essentials—Provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis
- CiscoView—Provides back- and front-panel displays; dynamic, color-coded graphical displays simplify device-status monitoring, device-specific component diagnostics, and application launching
- CiscoWorks Server—Provides the common management desktop services and security across the CiscoWorks Family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications
- Support for secure browser communications with CiscoView and RME sessions via Secure Socket Layer (SSL) and Secure Shell (SSH) protocol

Specifications

Feature	Description
Server	Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) IBM PC compatible with 550-MHz or higher Pentium III processor running (Dual processor system required for hosting multiple management solutions) Microsoft Windows 2000 Server or Professional Edition with Service Pack 2, Solaris 2.8
Client	IBM PC-compatible computer with 300-MHz or higher Pentium processor, Sun Ultra 10, HP9000 Series, IBM RS/6000 Windows NT 4 (Workstation and Server) with Service Pack 6a, Windows 98, 2000 Professional and Server with Service Pack 2; Solaris 2.7, 2.8; HP-UX 11.0; AIX 4.3.3 Internet Explorer v5.5 with Service Pack 2, 6.0; Netscape 4.76, 4.77, 4.78, 4.79
Supported Cisco Devices	Most Cisco IOS Software routers, access servers, hubs, and switches
Supported Cisco IOS Software Versions	Generally Cisco IOS Software Versions 10.3 and higher Catalyst Supervisor code 2.1 through 4.1 Note: Some CiscoWorks applications require certain versions of IOS and CAT these releases in order to operate, please see the specific application documentation and release notes for more information.

7926
E

Selected Part Numbers and Ordering Information[1]

LAN Management Solution	
CWLMS-2.1-K9	LAN Management Solution 21 for Windows and Solaris; includes Campus Manager 3.2, Device Fault Manager 1.2, Resource Manager Essentials 3.4, nGenius Real Time Monitor 1.4, CD One 5th Edition (Includes CiscoView 5.4)
CWLMS-2.1-P1-K9	Cross Bundle Discount LMS 2.1 for Windows and Solaris platforms; available to customers who have previously purchased RWAN 1.X and want to addLMS
LAN Management Solution Upgrades	
CWLMS-2.1-UP-K9	Upgrade kit for LMS 1.X customers wanting to upgrade to LMS 2.1; kit includes support for both Windows and Solaris platforms; primary value of this kit is to provide DFM to LMS 1.X customers
CWLMS-2.1-MR-K9	Maintenance kit for customers that purchased LMS 2.0 and want new device support and code updates; kit includes support for both Windows and Solaris platforms; includes updates to all LMS 2.X components (Should not be purchased by LMS 1.X customers)
CWLMS-1.2-MR-K9	Maintenance kit for customers that purchased LMS 1.X and want newdevice support and code updates to components in the 1.X release train; DFM is not included

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the LAN Management Solution Web site: **http://www.cisco.com/go/lms**

CiscoWorks VPN/Security Management Solution

CiscoWorks VPN/Security Management Solution (VMS), an integral part of the SAFE Blueprint for network security, combines Web-based tools for configuring, monitoring, and troubleshooting enterprise virtual private networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS). It offers the ability to monitor remote access links, and IPSec based site to site VPN's links. VMS is a Web-based solution that provides a "dashboard" view of critical VPN resources and their performance, VPN hardware and configuration and troubleshooting reports.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks VPN/Security Management Solution	• Complete management of a SAFEinfrastructure environment • Configuring andmonitoring VPN, PIX, IOS routers, and IDS devices. • Monitoring large remote access, and site-to-site hub and spoke VPNs from a single management console and focus on problem areas and performance.

Key Features

- Management and Monitoring Centers—Supplies the latest in management functionality and multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control. The management and monitoring centers include Management Center for PIX Firewalls, Management Center for IDS Sensors, Management Center for VPN Routers, and Monitoring Center for Security and Management center for PIX Firewalls (downloadable from CCO Software Center Fall 2002)
- VPN Monitor—Allows network administrators to collect, store, and view information on IPSec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser
- Cisco IDS Host Sensor Console—Provides real-time analysis and reaction to network hacking attempts by identifying an attack and preventing access to critical server resources before any unauthorized transactions occur

- Cisco Secure Policy Manager (CSPM)—Provides scalable, powerful policy-based security management system for Cisco firewalls and IPSec VPN routers which allows a customer to define, distribute, enforce, and audit network-wide security policies from a central location
- Resource Manager Essentials (RME)—Provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis
- CiscoView—Provides back- and front-panel displays; dynamic, color-coded graphical displays simplify device-status monitoring, device-specific component diagnostics, and application launching
- CiscoWorks Server—Provides the common management desktop services and security across the CiscoWorks family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications
- Support for secure browser communications with CiscoView and RME sessions via Secure Socket Layer (SSL) and Secure Shell (SSH) protocol

Specifications

Feature	CiscoWorks VPN/Security Management Solution
Server Hardware Requirements	IBM PC-compatible computerwith 1-GHz or faster Pentium processor Sun UltraSPARC 60 MP with 440-MHz or faster processor Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server)
Server Software Requirements	Windows 2000 Professional, Windows 2000 Server (Service Pack 2) Sun Solaris 2.7, 2.8
Client Hardware Requirements	IBM PC-compatible computer with 300-MHz or faster Pentium Solaris SPARCstation or Sun Ultra 10
Client Software Requirements	Windows 98, Windows NT 4.0, or Windows 2000 Server or Professional Edition with Service Pack 2 Solaris 2.7, 2.8
Browser Requirements	Internet Explorer 6.0 or 5.5 with Service Pack 2, on Windows 2000 Server or Professional Edition, Windows 98, and Windows NT 4.0. Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition and Windows98. Netscape Navigator 4.76 on Solaris 2.7, 2.8.

Selected Part Numbers and Ordering Information

CiscoWorks VPN/Security	Management Solution
CWVMS-2.1-UR-K9	CiscoWorks VMS 2.1 Windows and Solaris; Includes: Management Center for IDS Sensors, Management Center for VPN Routers, and Monitoring Center for Security, VPN Monitor 1.2, RME 3.4, CSPM 3.1, IDS Host Sensor 2.1, CD One 5th Edition[1]
CWVMS-2.1-WINR-K9	CiscoWorks VMS 2.1 Windows (20-Device Restricted License); Includes Management Center for IDS Sensors, Management Center for VPN Routers, and Monitoring Center for Security, VPN Monitor 1.2, RME 3.4, CSPM 3.1, IDS Host Sensor 21, CD One 5th Edition
CWVMS-2.1-URC-K9	Conversion from CiscoWorks VMS 2.1 for Windows (20-device Restricted License) to Unrestricted License (add Solaris Versions of CV, RME, VPN, and adds an unrestricted license to CSPM for Windows)[1]
CWVMS-2.1-UPGUR-K9	Upgrade from CSPM 2.x (Unrestricted License) to CiscoWorks VMS 2.1 for Windows and Solaris (Unrestricted License)[1]
CWVMS-2.1-WUPGR-K9	Upgrade from CSPM 2.X (Unrestricted License) to CiscoWorks VMS 2.1 for (20-device Restricted License)
CWVMS-2.1-UR-MR-K9	Maintenance rebase update for VMS 2.0 Windows and Solaris (Unrestricted License)[1]
CWVMS-2.1-R-MR-K9	Maintenance rebase update for VMS 2.0 Windows Only (20-device Restricted License)

[1] Contains Windows-only versions of CSPM and IDS Host Sensor

For More Information

See the CiscoWorks VPN/Security Management Solution Web site:
http://www.cisco.com/go/vms

7924
E

CiscoWorks IP Telephony Environment Monitor

CiscoWorks IP Telephony Environment Monitor (ITEM) is a bundled suite of management applications that helps ensure the manageability of converged networks that support Cisco IP telephony and IP telephony data applications. ITEM tracks the health of Cisco IP telephony environments by proactively monitoring the Cisco elements that support voice in the network to alert operations personnel of potential problems in order to minimize IP telephony service interruption.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks IP Telephony Environment Monitor	• Network managers who need to effectively manage their converged networks while maintaining high confidence that their IP telephony environments are performing as expected • Network Managers who need to use synthetic traffic (replicating key forms of network activity associated with VoIP and IP telephony) to enable around-the-clock monitoring of key voice elements in the network

Key Features

- Cisco Voice Health Monitor (VHM)—tracks the health of Cisco IP telephony environments by proactively monitoring Cisco voice elements in the network to alert operations personnel to potential problems and helps to minimize IP telephony service in network downtime. VHM leverages and requires the services of DFM while providing sophisticated capabilities of its own to ensure timely information on the health of IP telephony environments
- Cisco Device Fault Manager (DFM)—DFM provides real-time fault detection and determination about the underlying Cisco IP fabric on which the IP telephony implementation executes. DFM reports faults that occur on Cisco network devices, often identifying problems before users of network services realize that a problem exists
- CiscoView—CiscoView is a web-based graphical device-management technology and is the standard for managing Cisco devices, and providing back and front panel displays. Features include: Real-time monitoring of key information relating to device performance, traffic, and usage, with metrics such as utilization percentage, frames transmitted and received, errors, and a variety of other device-specific indicators

Optional Drop-In Modules

Fault History Manager

Fault History is an optional drop-in module (downloadable from CCO) that provides a web-based tool to access historical fault and alert data from a database. The user has several filtering options that can facilitate the search for specific information.

IP Phone Information Utility

The IP Phone Information Utility is an optional drop-in module (downloadable from CCO) that provides a web-based tool to show detailed information about individual IP telephone. The operator can access the IP phone information by using its extension number, IP address, and/or MAC address. This utility bases its information on the devices created in VHM.

IP Phone Help Desk Utility

The IP Phone Help Desk Utility is an optional applet (downloadable from CCO) that provides a MS Windows 2000 desktop tool to show summary information about individual IP telephone. The help desk operator can access the IP phone information by using its extension number (or can configure the application to search by IP or MAC addresses). This utility requires a connection to an ITEM server running VHM with the IP Phone Information Utility installed.

Gateway Statistics Utility

When available, the Gateway Statistics Utility is an optional drop-in module (downloadable from CCO) that provides a web-based tool to collect performance and behavior statistics about CCM-controlled IP telephony gateways. This statistical information can be subsequently exported for processing by reporting packages for capacity planning and trending information.

Specifications

Feature	CiscoWorks IP Telephony Environment Manager
Server Hardware	IBM PC-compatible wth 1 GHz or higher Pentium IV processor UNIX (If DFM is on Unix platform; Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) (Dual processor system required for hosting multiple management solutions)
Server Software	Windows 2000 Server or Professional Edition with Service Pack 2 Solaris 2.8
Client	IBM PC-compatible computer with 300 MHz or higher Pentium processor Windows NT 4 (Workstation & Server) with Service Pack 6a, Win 98 or Windows 2000 Professional & Server with Service Pack 2 Windows 98/NT/2000: Netscape v4.77, 4.78, 4.79 Windows 98/NT/2000: Internet Explorer v5.5 with Service Pack 2, 6.0

Selected Part Numbers and Ordering Information

CiscoWorks IP Telephony Environment Monitor

CWITEM-1.3-WIN-K9	CiscoWorks IP Telephony Environment Manager 1.3 for Windows Add-On for existing LMS 2.X and DFM 1.1 customers; includes VHM only
CWITEM-1.3-WIN-UP	CiscoWorks VoIP Health Monitor 1.0 Add-On for existing LMS 2.0 and DFM 1.1 customers; includes VHM only
CWITEM-1.3-MR-K9	Maintenance kit for customers that purchased CiscoWorks VoIP Health Monitor 1.0 and now want the new ITEM 1.3 device support and minor updates; kit includes support for Windows platforms only; includes updates to all components

For More Information

See the CiscoWorks IP Telephony Environment Monitor Web site at:
http://www.cisco.com/go/cwvoip

CiscoWorks Voice Manager for Voice Gateways

CiscoWorks Voice Manager for Voice Gateways (CVM) is a client-server, web-based voice management and reporting solution. The application provides enhanced capabilities to configure and provision voice ports, and create and modify dial plans on voice-enabled Cisco routers for voice over IP (VoIP), voice over Frame Relay (VoFR), and voice over ATM (VoATM) network deployments.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks IP Telephony Environment Monitor	• Network managers who need to maintaina distributed network architecture for increased scalability • Network Managers who need to manage multiple customernetworks from one common server

7922
3

Key Features

- Web interface management of voice ports and dial plan generation and management—Create and manage local dial plans and VoIP, VoFR, and VoATM network dial plans
- Report generation—Enhance graphical reporting capabilities with the software provided by an alliance with Telemate.Net (WIndows NT), a leading developer of enterprise information management tools; optional capabilities for enhanced reports, custom report creation, and multiple data source record collection exists.
- Optional capabilities to provide reporting on other data sources such as private branch exchanges (PBXs) and selected firewalls
- CiscoView—CiscoView is a web-based graphical device-management technology and is the standard for managing Cisco devices, and providing back and front panel displays. Features include: Real-time monitoring of key information relating to device performance, traffic, and usage, with metrics such as utilization percentage, frames transmitted and received, errors, and a variety of other device-specific indicators

Specifications

Feature	CiscoWorks Voice Manager for Voice Gateways
Server Hardware Requirements	256 MB of memory; 8-GB available hard disk space CPU running at 450 MHz (for WindowsNT) Sun Sparc/Ultra @333 MHz (for Solaris)
Server Software Requirements	Windows NT 4.0 with Service Pack 5 CiscoWorks CD One 4th Edition for WindowsNT
Client Hardware Requirements	64 MB of memory CPU running at 300 MHz
Client Software Requirements	Windows 95 running Netscape4.04 or Internet Explorer 4.01 and 64 MB of virtual memory Windows NT running Netscape 404 or Internet Explorer 4.01 and 64 MB of virtual memory Solaris running Netscape 404 with Telnet and Java enabled and 64 MB of virtual memory

Selected Part Numbers and Ordering Information[1]

CiscoWorks Voice Manager for Voice Gateways 2.1 9

CWVM-2.1	Voice Manager 2.1 for Windows & Solaris; includes Voice Manager 21 and CD One 4th Edition (CiscoView 5.3 and the October2001 Java patch update)
CWVM-2.1-UPG	Upgrade kit for CWVM 1.X customers wanting to upgrade to CVM 2.1; kit includes support for both Windows and Solaris platforms
CWVM-2.1-UPT	Minor updates to CWVM 2.1 for Windows and Solaris from CWVM 2.X; update includes support for both Windows and Solaris platforms

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Voice Manager for Voice Gateways Web site at:
http://www.cisco.com/go/cw2kvm

CiscoWorks QoS Policy Manager

QoS Policy Manager allows you to centrally define and administer IOS and CAT parameters needed for differentiating network traffic. This ensures high availability and predictable performance for business-critical which rely on advanced voice and video services. Cisco QoS Policy Manager (QPM) 3.0 is a key enabler of end-to-end QoS for converged networks. It delivers differentiated services across network infrastructures with converged voice, video, and data applications, simply by taking advantage of Cisco IOS and Catalyst OS Software with built-in QoS mechanisms in LAN and WAN switching and routing equipment.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco QoS Policy Manager	• End-to-end QoS configurationand automated, reliable policy deployment while eliminating device-by-device command streams • Rules-based policiesthat combine static and dynamic port applications and host system traffic filters • QoS Policy Manager's services, including congestion management & avoidance, and traffic-shaping • Efficientlytranslate polcies to specific QoS config commands,ensuring consistency across domains • Validate polcies prior to deploying them quickly and reliably to LAN and WAN policy domains • Generate Web-based reportson QoS policiesdeployed in the network

Key Features

- Provides baseline monitoring which profiles traffic by top applications and a small number of classes before QoS deployment
- Validates QoS deployments by obtaining detailed feedback on traffic patterns after QoS at different points in the network
- Provides statistics related to QoS policies which include traffic matching NBAR filters and action statistics
- Supports CBQoSMIB and CAR MIB
- IP Telephony templates provide pre-defined QoS policies that ensure strict priority for voice traffic in Enterprise networks
- Delivers the appropriate service-level to business-critical applications by supporting the extension of IP packet classification to include application signature, Web URLs, and negotiated ports
- Extend security by defining access control policies to permit or deny transport of packets into or out of device interfaces
- Allows QoS policy validation checking, uploading of existing device configuration, previewing configuration changes, incremental ACL updates, and managing policy distribution

Specifications

Feature	Cisco QoS Policy Manager
Server Hardware Requirements	IBM PC-compatible computerwith 1-GHz or faster Pentium processor Sun UltraSPARC 60 MP with 440-MHz or faster processor Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server)
Server Software Requirements	Windows 2000 Professional, Windows 2000 Server (Service Pack 2) Sun Solaris 2.7, 2.8
Client Hardware Requirements	IBM PC-compatible computer with 300-MHz or faster Pentium Solaris SPARCstation or Sun Ultra 10Complete
Client Software Requirements	Windows 98, Windows NT 4.0, or Windows 2000 Server or Professional Edition with Service Pack 2 Solaris 2.7, 2.8
Browser Requirements	Internet Explorer 6.0 or 5.5 with Service Pack 2, on Windows 2000 Server or Professional Edition, Windows 98, and Windows NT 4.0. Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition and Windows 98. Netscape Navigator 4.76 on Solaris 2.7, 2.8.

Selected Part Numbers and Ordering Information[1]

Cisco QoS Policy Manager	
CWQPM-3.0-WINUR-K9	QoS Policy Mgr 3.0 for Windows (Unrestricted License)
CWQPM-3.0-WINR-K9	QoS Policy Mgr 3.0 for Windows (20- Device Restricted License)
CWQPM-3.0-URUP-K9	Upgrade to QPM 3.0 for Windows from QPM 1.x or 2.x to QPM 3.0 unrestricted
CWQPM-3.0-URC-K9	Conversion of a QPM 3.0 20-device restricted usage license to unrestricted deviceusage license

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

7920
3

For More Information

See the Cisco QoS Policy Manager Web site: **http://www.cisco.com/go/qpm**

Cisco Ethernet Subscriber Solution Engine

The Cisco Ethernet Subscriber Solution Engine (ESSE) is a hardware-based management system for metro access networks that use the Cisco ONT 1000 Gigabit Ethernet Series Optical Network Terminator. The Cisco ESSE enables complete remote management and troubleshooting of the customer demarcation point for Ethernet over fiber. Remote management and diagnostics reduce operating expenses and increase profitability by eliminating the need for unnecessary visits to the customer premises. The Cisco ESSE runs on the Cisco 1105, which is one rack unit (1RU) high, enabling you to conveniently deploy the Cisco ESSE on the same rack with the rest of your Cisco metro Ethernet network aggregation equipment.

The Cisco ESSE automatically discovers all Cisco ONT 1000 Gigabit Ethernet Series devices in the metro access network, applies the designated configuration, and instantly begins collecting statistics and management information.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Ethernet Subscriber Solution Engine	The Cisco Ethernet Subscriber Solution Engine is ideal for service providers seeking to: • Reduce operating expenses byimplementingmetro accessnetworkswith Ethernet over fiber • Reduce customeronsite visits, which are time-consuming and expensive • Perform complete remote configuration and troubleshooting of the Cisco ONT 1000 Gigabit Ethernet Series

Key Features

- Enables service providers to perform remote control of inventory, configuration, statistics, fault management, and troubleshooting on the Cisco ONT 1000 Gigabit Ethernet Series
- Full Layer 1 and Layer 2 remote configuration and monitoring of Optical Network Terminators
- Access to all Ethernet port registers and statistics on the Cisco ONT 1000 Gigabit Ethernet Series
- Easy identification of ONTs with searchable, user-defined properties such as customer name, VLAN ID, and street address

Selected Part Numbers and Ordering Information[1]

Cisco Ethernet Subscriber Solution Engine

CESSE-1105-K9	Cisco Ethernet Subscriber Solution Engine; Includes the Cisco 1105 hardware platform and Ethernet Subscriber management software, version 1.1

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Ethernet Subscriber Solution Engine Web site:
http://www.cisco.com/go/esse

CiscoWorks Wireless LAN Solution Engine

The CiscoWorks WLSE is a specialized, daily operational solution that allows customers to manage the entire Cisco Aironet WLAN infrastructure. It offers powerful, centralized template-based configuration with user-defined device groups to efficiently configure large numbers of access points and bridges. The CiscoWorks WLSE provides centralized firmware updates to facilitate firmware changes throughout the WLAN. It monitors Access Control Server (ACS) authentication servers, supports both Cisco Extensible Authentication Protocol (LEAP) and generic RADIUS servers, and further enhances security management by detecting misconfigurations on access points and bridges. The CiscoWorks WLSE proactively monitors WLAN infrastructures and generates notifications for unavailability and performance degradation. The CiscoWorks WLSE aids in capacity planning by identifying the most used access points, and accelerates troubleshooting by generating client association reports.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Wireless LAN Solution Engine	The CiscoWorks WLSE is ideal for enterprise customers: • Implementing large-scale Cisco Aironet WLAN infrastructures • Template-based configuration tool which can include a large number of uniform policies for Cisco access points and bridges • Access point and bridge mis-configuration alerts to minimize security vulnerabilities • Proactive fault and performance monitoring of Cisco access points, bridges, LEAP authentication server, and switches connected to theaccess points

Key Features

- Centralized template-based configuration with hierarchical, user-defined groups
- Plug and play configuration of newly deployed access points and bridges
- Centralized firmware update to facilitate firmware changes
- Access point and bridge misconfiguration alerts to minimize security vulnerabilities
- Proactive monitoring of access points, bridges, ACS authentication servers (both LEAP and generic RADIUS), and the switches connected to the access points
- Configuration and monitoring of virtual LAN (VLAN) and quality of service (QoS) on access points to maximize security and performance
- Access point usage, summary, and client association reports with XML, CSV, and PDF data export
- Secure HTML-based user interface for easy access anywhere
- Upper-layer network management system and operations support system (NMS/OSS) integration with syslog message, SNMP trap, and e-mail notifications

Selected Part Numbers and Ordering Information[1]

CiscoWorks Wireless LAN Solution Engine

CWWLSE-1105-K9	Wireless LAN Solution Engine1.0; includes the Cisco 1105 hardware platform and wireless LAN management software version 1.0

7918
3

For More Information

See the CiscoWorks Wireless LAN Solution Engine Web site: **http://www.cisco.com/go/wlse**

CiscoWorks Hosting Solution Engine

CiscoWOrks Hosting Solution Engine is a network management appliance that monitors, activates, and configures a variety of e-business services in Cisco powered data centers. It provides up-to-date fault and performance information about the network infrastructure and Layer 4-7 network services.

HSE automatically discovers the entire data center infrastructure and instantly begins collecting statistics and management information, providing a current snapshot of the managed environment. HSE provides up-to-date information for operational staff to easily pinpoint the source of a problem. HSE itself is a manageable Cisco device with a full Cisco Discovery Protocol implementation and supports Cisco MIB II.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Hosting Solution Engine	• Ideal for enterprise and service providers with e-business data center facilties • Granular user access model to partition network resources for Layer 4-7 services and switch ports, and authorize user group access to individual application services • Robust Layer 4-7 service configuration and service activation of server load balancing devices, including virtual servers, real servers, and content ownersand rules

Key Features

- Granular user access to partition network resources for Layer 4-7 services as well as switch ports; authorize user group access to individual application services
- Robust Layer 4-7 service configuration and service activation of content switches
- Monitoring and reporting of SSL Proxy services on Cisco Catalyst 6000 Series with SSL Service Modules and Cisco Content Services Switch
- Flexible fault and performance monitoring of Cisco routers, switches, Cisco PIX® Firewalls, Cisco Content Engines, Cisco Content Switches and L4-7 services
- HTML-based, secure graphic user interface with easy customer view/report personalization and historical data reporting
- Upper layer NMS/OSS integration with SYSLOG, trap, email notifications and historical data XML export

Selected Part Numbers and Ordering Information[1]

Cisco 1105 Hosting Solution Engine

CWHSE1105-1.5-K9	CiscoWorks Hosting Solution Engine; includes 1105 hardware platform with software version 1.5; can be configured for internationalpower cords

[1] Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the 1105 Hosting Solution Engine Web site: **http://www.cisco.com/go/1105hse**

Cisco Catalyst 6500 Series Network Analysis Module 1 and 2(with NAM software version 2.2)

The Cisco Network Analysis Module (NAM) 1 and 2, second generation high performance network analysis modules for the Cisco Catalyst 6500 Series provides network monitoring instrumentation and web-browser based traffic analysis for Catalyst based AVVID environments. The NAM enables network managers to gain application-level visibility into network traffic with the ultimate goal of improving performance, reducing failures, and maximizing returns on network investment. The new NAMs are available in two hardware versions, NAM-1 and NAM-2, to meet diverse network analysis needs in a scalable switching environment running up to gigabit speeds. The NAMs come with an embedded, Web-based traffic analyzer, which provides full scale remote monitoring and troubleshooting capabilities that are accessible through a Web browser.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 6500 Series Network Analysis Module 1 and 2 (with NAM software version 2.2)	• Needs Application-Level visibility built into the network • Provides network managers visibility into all layers of network traffic • Monitoring in a scalable switching environment that supports traffic monitoring in a scalable switching environment • Offers investment protection by interfacing with both the bus and the crossbar switching fabric-based architectures in the Cisco Catalyst 6500 Series

Key Features

- Provides application-level Remote Monitoring (RMON) functions based on RMON2 and other advanced Management Information Bases (MIBs)
- Collects statistics on both data and VoIP streams flowing through the host switch using the Switch Port Analyzer (SPAN) and NetFlow Data Export features of the Cisco Catalyst 6500 Series
- Collects data from remote switches using the remote SPAN (RSPAN) feature of the Cisco Catalyst 6500 and 4000 Series switches
- Easy to deploy and use at LAN aggregation where they can see most of the traffic, at service points where performance is critical and at important access points where quick troubleshooting is required
- Application monitoring can be done using RMON, RMON2, and several extended RMON MIBs, which can detect the applications on the network and provide detailed information about how these applications utilize the bandwidth, which hosts access those applications, and which client/server pairs generate the most traffic
- Performance management provides valuable information about the delays in server responses to client requests

Selected Part Numbers and Ordering Information[1]

Cisco Catalyst 6500 Series Network Analysis Module 1 and 2(with NAM software version 2.2)

WS-SVC-NAM-1	Catalyst 6500 Series Network Analysis Module 1. To order the NAM individually, please use the spare part number of WS-SVC-NAM-1=
WS-SVC-NAM-2	Catalyst 6500 Series Network Analysis Module 2. To order the NAM individually, please use the spare part number of WS-SVC-NAM-2=

[1] Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco NAM Web site: **http://www.cisco.com/go/6000nam**

AP GB

Cisco Systems

Data Sheet

Cisco **1751** Modular Access Router

Cisco 1751 Modular Access Router is ideally suited to help you evolve your organization into an e-Business. It supports e-Business features such as VPNs; secure Internet, intranet, and extranet access with optional firewall technology; broadband DSL and cable connectivity; and multiservice voice/video/data/fax integration. The Cisco 1751 Modular Access Router offers:

- Flexibility to adapt to changing requirements
- Modularity that allows you to individually configure the system to meet specific business needs
- Investment protection with features and performance to support new WAN services such as broadband DSL and cable access, multiservice voice/data integration, and VPNs
- Integration of multiple network functions, including an optional firewall VPN, and data service unit/channel service unit (DSU/CSU) to simplify deployment and management

The Cisco 1751 Router delivers these capabilities with the power of Cisco IOS Software in a modular integrated access solution. The Cisco 1751 Router provides a cost-effective solution to support e-Business applications through a comprehensive feature set including support for:

- Multiservice voice/fax/data integration
- Secure Internet, intranet, and extranet access with VPN and firewall
- Integrated broadband DSL connectivity
- VLAN support (IEEE 802.1Q)

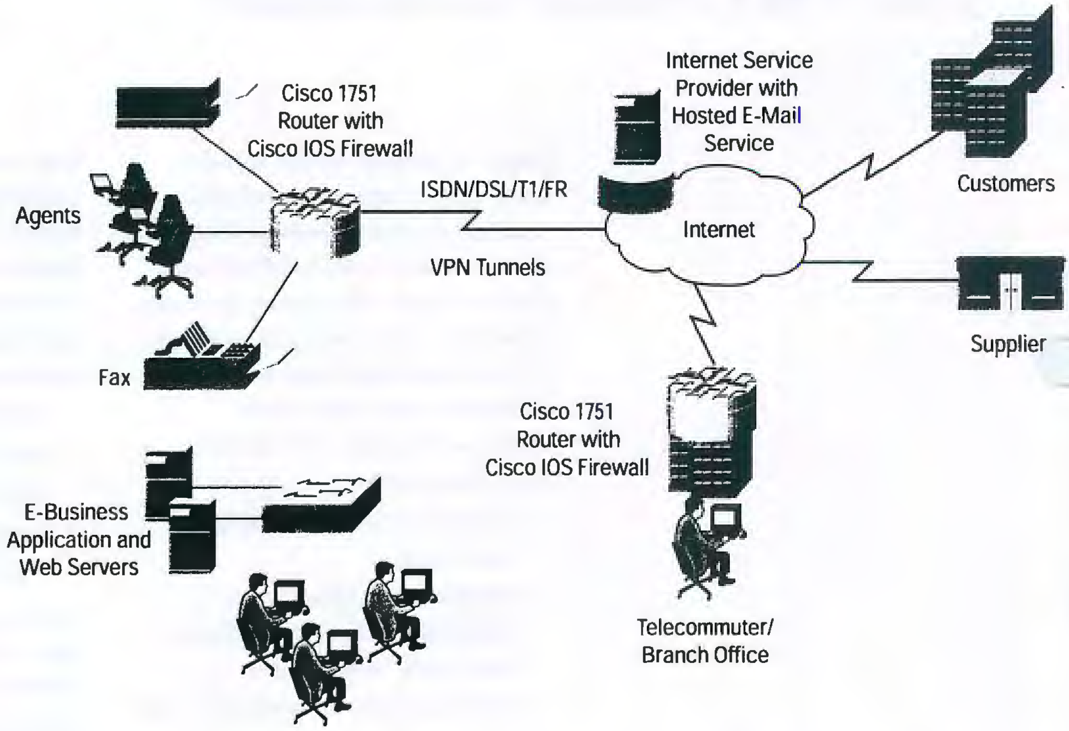
The Cisco 1751 Router, a member of the Cisco 1700 Family, features a modular architecture that enables cost-effective upgrades and additions of WAN and voice interfaces. Integrated network services and functions, such as optional firewall, DSU/CSU, and VPN features, reduce the complexity of deploying and managing e-Business solutions. The Cisco 1751 Router offers investment protection when your business needs it, with a RISC architecture and features to support new technologies and applications such as voice/video/data/fax integration and VPNs. See Figure 2.

Figure 1

The Cisco 1751 Router delivers a versatile e-Business WAN access solution.

Figure 2

Cisco 1751 Routers provide all necessary capabilities to connect to the Internet and communicate with vendors, customers, and other employees and offices.



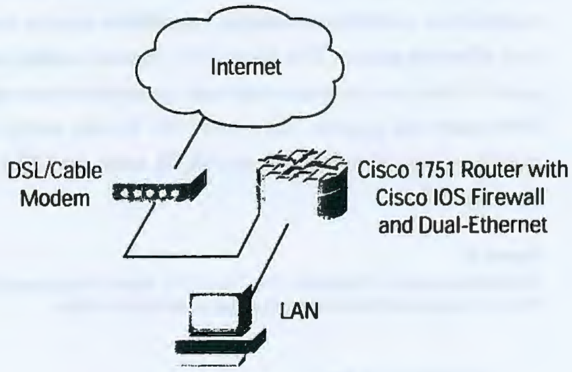
The Cisco 1751 Router is available in two models that enable you to easily tailor an access solution to suit your e-Business requirements today and in the future. See Table 1.

Table 1 The Cisco 1751 Modular Access Router

Cisco 1751 **Base Model**	Includes everything an office needs for data networking now (16 MB Flash, 32 MB DRAM, and Cisco IOS IP software feature set), with a simple upgrade path to full voice functionality. WAN interface cards are available separately.
Cisco 1751-V **Multiservice Model**	Includes all the features needed for immediate integration of data and voice services with support for up to two voice channels (32 MB Flash and 64 MB DRAM, one DSP (PVDM-256K-4), and Cisco IOS IP Plus Voice feature set). Voice and WAN interface cards are available separately.

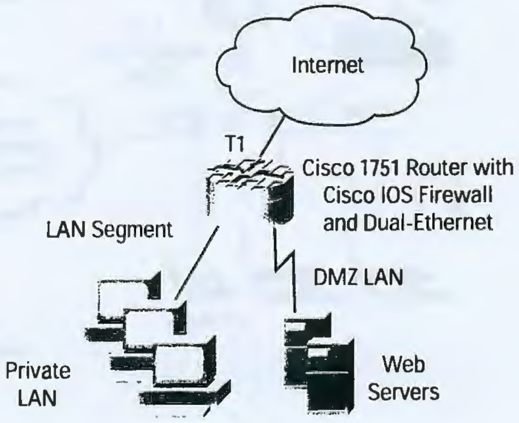
All Cisco 1751 models offer three modular slots for voice and data interface cards, an autosensing 10/100BaseT Fast Ethernet LAN port supporting standards-based IEEE 802.1Q VLAN, a console port, and an auxiliary port. The Cisco 1751 Router supports the same WAN interface cards as the Cisco 1600, 1700, 2600, and 3600 Series routers, and the same voice interface cards and voice-over-IP (VoIP) technology as the Cisco 1700, 2600, and 3600 Series routers. This simplifies support requirements. The WAN interface cards support a wide range of services, including synchronous and asynchronous serial, Integrated Services Digital Network Basic Rate Interface (ISDN BRI), ADSL, and serial with DSU/CSU options for primary and backup WAN connectivity. The voice interface cards support Foreign Exchange Office (FXO), Foreign Exchange Station (FXS), Network and User Side Voice BRI (ISDN BRI NT/TE), Ear & Mouth (E&M), direct inward dial (DID), and T1/E1 Multiflex VWICs. Additionally, an Ethernet interface card provides the Cisco 1751 Router with dual-Ethernet capability to support the external broadband modem devices. See Figure 3.

Figure 3
Cisco 1751 Router Incorporating Ethernet WAN Interface Card (WIC) Deployed with Broadband Modem



In addition, dual-Ethernet capability on the Cisco 1751 Router enables the creation of perimeter/DMZ (demilitarized zone) LANs to enhance security by physically separating private and public data. See Figure 4.

Figure 4
Cisco 1751 Router Incorporating Ethernet WIC to Deploy Perimeter/DMZ LAN



Combined, these interfaces support a comprehensive set of applications, including multiservice voice/video/data/fax integration, Frame Relay, ISDN BRI, SMDS, X.25, broadband DSL and cable services, and VPNs.

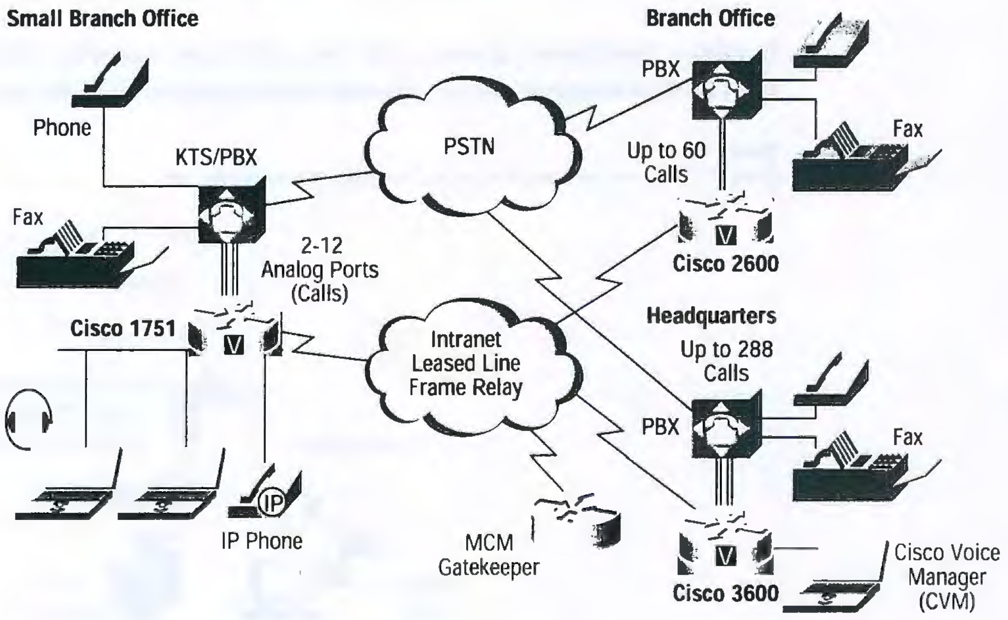
Key Benefits

The Cisco 1700 Series routers support the value of end-to-end Cisco network solutions with the following benefits:

Flexibility—The modular Cisco 1751 Router adapts easily to fit the needs of growing businesses. Interchangeable WAN interface cards enable easy additions or changes in WAN technologies without requiring a forklift upgrade of the entire platform. Modular data and voice slots enable users to tailor data and voice services as needed. With the ability to use the same field-upgradable WAN and voice interface cards across multiple Cisco access router platforms, the Cisco 1751 Router reduces requirements for spare parts inventory and support training.

Multiservice Access—For businesses that want to become e-Businesses and incorporate applications that integrate multiservice voice/video/data/fax capabilities now or in the future, the Cisco 1751 Router offers a flexible, cost-effective answer. The Cisco 1751 Router enables network managers to save on long-distance interoffice billing costs. It also interoperates with next-generation voice-enabled applications such as integrated messaging and Web-based call centers. The Cisco 1751 Router works with the existing telephone infrastructure—phones, fax machines, key telephone systems (KTS) units, and PBX (including digital PBXs)—minimizing capital costs. See Figure 5.

Figure 5
Voice/video/data/fax integration. The Cisco 1751 Router integrates data and voice capabilities, significantly lowering toll charges for small- and medium-sized businesses and enterprise small branch offices.



Lower Cost of Ownership—The Cisco 1751 Router provides a complete solution for integrated voice and data access in a single product, eliminating the need to install and maintain a large number of separate devices. You can combine optional functions—including a voice gateway, dynamic firewall, VPN tunnel server, DSU/CSU, ISDN network termination-1 (NT1) device, and more—to reduce deployment and management costs. This solution can be managed remotely using network management applications such as CiscoWorks2000 and CiscoView or any SNMP-based management tool.

Investment Protection—The Cisco 1751 Router RISC architecture, Cisco IOS Software, and modular slots provide solid investment protection. The Cisco 1751 incorporates services such as multiservice voice/video/data/fax integration, VPNs, and broadband DSL and cable communications to enable today's successful e-Business. An internal expansion slot on the mother- board offers the ability to support hardware-assisted IPSec data encryption at T1/E1 speeds.

For a complete list of Cisco 1751 Router features and benefits, see Table 2.

Table 2 Key Features and Benefits

Features	Benefits
Flexibility	
Full Cisco IOS Software support, including multiprotocol routing (IP, IPX, Apple Talk, IBM/ SNA) and bridging	• Provides the industry's most robust, scalable, and feature-rich internetworking software support using the de facto standard networking software for the Internet and private WANs • Part of the Cisco end-to-end network solution
Integrated Voice and Data Networking	
Cisco 1751 router chassis accepts both WAN and voice interface cards	• Reduces long-distance toll charges by allowing the data network to carry interoffice voice and fax traffic • Works with existing handsets, key units, and PBXs, eliminating the need for a costly phone-equipment upgrade
Modular Architecture	
Accepts an array of WAN and voice interface cards	• Adds flexibility and investment protection
WAN interface cards and voice interface cards are shared with Cisco 1600, 1700, 2600, and 3600 routers	• Reduce cost of maintaining inventory • Lower training costs for support personnel • Protect investments through re-use on various platforms
Autosensing 10/100 Fast Ethernet	• Simplifies migration to Fast Ethernet performance in the office
Expansion Slot on Motherboard	• Allows expandability to support hardware-assisted encryption at T1/E1 speeds • Allows support for future technologies
Dual DSP Slots	• Allow expandability to support additional voice channels
Security	
The Cisco IOS Firewall Feature Set includes context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, Java blocking, real-time alerts, Intrusion Detection System (IDS), and encryption	• Allows internal users to access the Internet with secure, per-application-based, dynamic access control, while preventing unauthorized Internet users from accessing the internal LAN

Table 2 Key Features and Benefits (Continued)

Features	Benefits
IPSec DES and 3DES	• Enable creation of VPNs by providing industry-standard data privacy, integrity, and authenticity as data traverses the Internet or a shared public network • Supports up to 168-bit encryption
Hardware-Based Encryption Using Optional VPN Module	• Supports wire-speed encryption up to T1/E1 speeds
Device Authentication and Key Management	
IKE, X.509v3 digital certification, and support for certificate enrollment protocol (CEP) with certification authorities (CAs) such as Verisign and Entrust	• Ensure proper identity and authenticity of devices and data • Enable scalability to very large IPSec networks through automated key management
User Authentication	
PAP/CHAP, RADIUS, TACACS+	• Support all leading user identity verification schemes
VPN Tunneling	
IPSec, GRE, L2TP, L2F	• Offer choice of standards-based tunneling methods to create VPNs for IP and non-IP traffic • Allow standards-based IPSec or L2TP client to interoperate with Cisco IOS tunneling technologies • Fully interoperable with public certificate authorities and IPSec standards-based products • Part of the scalable Cisco end-to-end VPN solution portfolio
Cisco Easy VPN client	• Allows the router to act as remote VPN client and have VPN policies pushed down from the VPN concentrator
Cisco Unified VPN Access Server	• Allows the router to terminate remote access VPNs initiated by mobile and remote workers running Cisco VPN client software on PCs; and allows the router to terminate site-site VPNs initiated by IOS routers using the Cisco Easy CPN client feature
Management	
IEEE 802.1Q VLAN Support	• VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical LAN infrastructure into different subnets
Manageable via SNMP (CiscoView, CiscoWorks2000), Telnet, and console port	• Allow central monitoring, configuration, and diagnostics for all functions integrated in the Cisco 1751 router, reducing management time and costs
Cisco SDM	• Simplifies router and security configuration through smart wizards to enable customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI)

Table 2 Key Features and Benefits (Continued)

Features	Benefits
Ease of Use and Installation	
Cisco ConfigMaker, SETUP configuration utility, AutoInstall, color-coded ports/cables, and LED status indicators	• Simplifies and reduces deployment time and costs with graphical LAN/VPN policy configurator; command-line, context-sensitive configuration questions; and straightforward cabling • LEDs allows quick diagnostics and troubleshooting
Network Address Translation (NAT) and Easy IP	• Simplifies deployment and reduces Internet access costs
QoS	
CAR, Policy Routing, WFQ, PQ/CBWFQ, GTS, RSVP, DSCP, cRTP, MLPPP and LFI	• Allocates WAN bandwidth to priority applications for improved performance
Reliability and Scalability	
Cisco IOS Software, dial-on-demand routing, dual-bank Flash memory, scalable routing protocols such as OSPF, EIGRP, and HSRP	• Improves network reliability and enables scalability to large networks
Broadband Connectivity Options	
ADSL and cable connectivity deliver business-class broadband access	• Leverage broadband access technologies like cable and DSL to increase WAN connectivity speeds and reduce WAN access costs • The Cisco 1751 supports ADSL connectivity with ADSL WIC • Cable connectivity with the Cisco 1751 and optional integrated Cisco uBR910 Series Cable DSU deliver business-class broadband access
Device Integration	
Integrated router, voice gateway, firewall, encryption, VPN tunnel server, DSU/CSU, and NT1 in a single device	• Reduce costs and simplifies management

Cisco IOS Technology

Internet and Intranet Access

Cisco IOS Software provides an extensive set of features that make the Cisco 1751 Router ideal for flexible, high-performance communications across both intranets and the Internet:

- Multiprotocol routing (IP, IPX, and AppleTalk), IBM/SNA, and transparent bridging over ISDN, asynchronous serial, and synchronous serial such as leased lines, Frame Relay, SMDS, Switched 56, X.25, and X.25 over ISDN D
- WAN optimization—including dial-on-demand routing (DDR), bandwidth-on-demand (BOD) and OSPF-on-demand circuit, Snapshot routing, compression, filtering, and spoofing to reduce WAN costs

Security

Cisco IOS Software supports an extensive set of basic and advanced network security features, including access control lists (ACLs); user authentication, authorization, and accounting (such as PAP/CHAP, TACACS+, and RADIUS); and data encryption. To increase security, the integrated Cisco IOS Firewall Feature Set protects internal LANs from attacks with context-based access control (CBAC) and Intrusion Detection (IDS), while IPSec tunneling with data encryption standard DES and 3DES encryption provide standards-based data privacy, integrity, and authenticity as data travels through a public network. Additionally, remote management applications, such as Cisco Security Device Manager (SDM), make it easier than ever to deploy and monitor security applications on your Cisco router.

The Cisco 1700 Series routers support the Cisco Easy VPN client feature that allows the routers to act as remote VPN clients. As such, these devices can receive predefined security policies from the headquarters' VPN head-end, thus minimizing configuration of VPN parameters at the remote locations. This solution makes deploying VPN simpler for remote offices with little IT support or for large deployments where it is impractical to individual configure multiple remote devices. While customers wishing to deploy and manage site-to-site VPN would benefit from Cisco Easy VPN client because of its simplification of VPN deployment and management, managed VPN service providers and enterprises who must deploy and manage numerous remote sites and branch offices with IOS routers for VPN will realize the greatest benefit.

The Cisco 1700 Series routers also support the Cisco Unified VPN Access Server feature that allows a Cisco 1700 router to act as a VPN head-end device. In site-to-site VPN environments, the Cisco 1700 router can terminate VPN tunnels initiated by the remote office routers using the Cisco Easy VPN client. Security policies can be pushed down to the remote office routers from the Cisco 1700 Series routers. In addition to terminating site-to-site VPNs, a Cisco 1700 Series router running the Unified VPN Access Server can terminate remote access VPNs initiated by mobile and remote workers running Cisco VPN client software on PCs. This flexibility makes it possible for mobile and remote workers, such as sales people on the road, to access company intranet where critical data and applications exist.

For remote access, VPNs, Layer 2 Forwarding (L2F), and Layer 2 Tunneling Protocol (L2TP) combine with IPSec encryption to provide a secure multiprotocol solution for IP, IPX, and AppleTalk traffic, and more. Mobile users can dial in to a service provider's local point of presence (POP) and data is "tunneled" (or encapsulated inside a second protocol such as IPSec or L2TP) back to the Cisco 1751 router to securely access the corporate network via the Internet.

Cisco IOS Software QoS Features

Through Cisco IOS Software, the Cisco 1751 Router delivers quality of service (QoS) capabilities, including Resource ReSerVation Protocol (RSVP), Weighted Fair Queuing (WFQ), Committed Access Rate (CAR), and IP Precedence. These features enable businesses to prioritize traffic on their networks by user, application, traffic type, and other parameters, to ensure that business-critical data and delay-sensitive voice are appropriately prioritized.

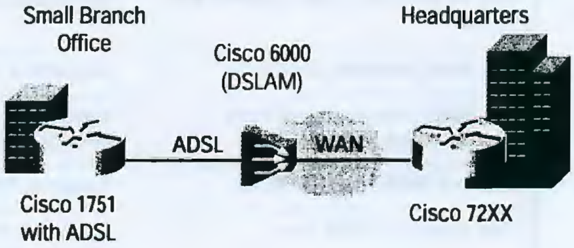
Because the Cisco 1751 Router provides robust voice compression, up to 8 voice calls can occupy a single 64K data channel simultaneously, without compromising data performance. Cisco IOS voice compression technology integrates data and voice traffic to enable efficient use of existing data networks.

High-Performance Architecture for VPNs and Broadband Service

A robust RISC architecture and Cisco IOS features enable the Cisco 1751 Router to support VPN applications with tunneling and security, as well as DSL, cable, and other broadband access technologies. An internal slot on the Cisco 1751 motherboard supports an optional VPN module that provides hardware-assisted IPSec DES and 3DES encryption at T1/E1 speeds. The Cisco 1751 Router equipped with the WIC-1ADSL supports VPN over ADSL service. See Figure 6. The Cisco 1751 Router with the uBR910 series cable DSU supports business-class broadband cable access. The Ethernet WIC (WIC-1ENET) provides an alternate method of deploying DSL/cable Internet access with the use of an external modem. In some cases, the ISP provides the broadband modem.

Figure 6

The Cisco 1751Router, deployed in conjunction with the ADSL WIC, enables SMB and small branch customers to reap the benefits of ADSL.



Network Management and Ease of Installation

The Cisco 1751 Router supports a range of network-management and ease-of-installation tools:

- The Cisco Security Device Manager (SDM) is an intuitive, web-based device management tool embedded within the Cisco IOS access routers. SDM simplifies router and security configuration through smart wizards to enable customers to quickly and easily deploy, configure and monitor a Cisco access router without requiring knowledge of Cisco IOS Command Line Interface (CLI). For more information visit www.Cisco.com/go/sdm.
- Cisco ConfigMaker is a Windows wizard-based tool designed to configure a small network of Cisco routers, switches, hubs, and other network devices from a single PC. This tool makes it easy to configure value-add security features such as the Cisco IOS Firewall Feature Set, IPSec encryption, and network address translation (NAT); establish VPN policies (including QoS and security); and configure the Dynamic Host Configuration Protocol (DHCP) server.
- CiscoWorks for Windows, a comprehensive network management solution for small to medium sized networks that provides Web-based network monitoring and device configuration management.
- CiscoWorks2000, the industry-leading Web-based network management suite from Cisco, simplifies tasks such as network inventory management and device change, rapid software image deployment, and troubleshooting.
- For service providers, Cisco Service Management (CSM) provides an extensive suite of service management solutions to enable planning, provisioning, monitoring, and billing.

Extending Cisco End-to-End Solutions

As part of the comprehensive Cisco end-to-end networking solution, the Cisco 1700 Series routers enable businesses to extend a cost-effective, seamless network infrastructure to the small branch office. The Cisco 1700 Family of access routers includes the Cisco 1751 Router and Cisco 1721 Router—a modular device optimized for data-only connections. WAN cards work with both devices, as well as with Cisco 1600, 2600, and 3600 Series routers. They are powered by Cisco IOS Software for robust WAN service between branches and central offices in organizations with multiple sites. Both feature RISC-based processors to provide performance for encryption and support for emerging broadband technologies.

The Cisco 1751 Router also shares VoIP technology and analog voice interface cards with Cisco 2600 and 3600 Series routers. This feature provides an end-to-end solution for multiservices communications between offices, simplifying inventory needs and leveraging IT expertise across more devices in an organization.

For a complete list of physical interfaces, see Tables 3, 4, 5, and 6.

Table 3 Physical Interfaces/Architecture

One 10/100 BaseT Fast Ethernet Port (RJ45)	Automatic speed detection; automatic duplex negotiation; VLAN support
One Voice Interface Card Slot	Supports a single voice interface card with two ports per card
Two WAN Interface Card/Voice Interface Card Slots	Supports any combination of up to two WAN interface cards or voice interface cards
Ethernet WAN Interface Cards	Supports PPP and PPPoE; operates in full and half-duplex modes
One Auxiliary (AUX) Port	RJ-45 jack with RS232 interface (plug compatible with Cisco 2500 Series AUX port); asynchronous serial DTE with full modem controls (CD, DSR, RTS, CTS); asynchronous serial data rates up to 115.2 kbps
One Console Port	RJ-45 jack with RS232 interface (plug compatible with Cisco 1000/1600/2500 series console ports); asynchronous serial DTE; transmit/receive rates up to 115.2 kbps (default 9600 bps, not a network data port); no hardware handshaking such as RTS/CTS
One Internal Expansion Slot	Supports hardware-assisted services such as encryption (up to T1/E1)
RISC Processor	Motorola MPC860P PowerQUICC at 48MHz

Table 4 WAN Support

Asynchronous Serial Interfaces on Serial WAN Interface Cards	Interface speed: up to 115.2 Kbps; asynchronous serial protocols: Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP); asynchronous interface; EIA/TIA-232
ISDN WAN Interface Cards	ISDN dialup and ISDN leased line (IDSL) at 64 and 128 Kbps; encapsulation over ISDN leased line; Frame Relay and PPP
ADSL WAN Interface Cards	Supports ATP adaption Layer 5 (AAL5) services and applications; interoperates with Alcatel DSLAM with Alcatel chipset and Cisco 6130/6260 DSLAM with Globespan chipset; ANSI T1.413 issue 2 and ITU 992.1 (G.DMT) compliant

Table 5 WAN Interface Cards for the Cisco 1751 Router

Module	Description
WIC-1T	One serial, async, and sync (T1/E1)
WIC-2T	Two serial, async, and sync (T1/E1)
WIC-2A/S	Two low-speed serial (up to 128 kbps), async, and sync
WIC-1B-S/T	One ISDN BRI S/T
WIC-1B-U	One ISDN BUI U with integrated NT1
WIC-1DSU-56K4	One integrated 56/64-kbps, four-wire DSU/CSU
WIC-1DSU-T1	One integrated T1/fractional T1 DSU/CSU
WIC-1ADSL	One-port ADSL interface
WIC-1ENET	One-port 10BaseT Ethernet Interface
WIC-1SHDSL	One-port G.SHDSL interface
WIC-1AM	One-port V.90 analog modem WIC
WIC-2AM	Two-portV.90 analog modem WIC

Table 6 Voice Interface Cards for the Cisco 1751

VIC-2FXS	Two-port FXS voice/fax interface card for voice/fax network module
VIC-2DID	Two-port DID (direct inward dial) voice/fax interface card
VIC-2FXO	Two-port FXO voice/fax interface card for voice/fax network module
VIC-2FXO-EU	Two-port FXO voice/fax interface card for Europe
VIC-2FXO-MI	Two-port FXO voice/fax interface card with battery reversal detection and Caller ID support (for US, Canada, and others) [enhanced version of the VIC-2FXO]
VIC-2FXO-M2	Two-port FXO voice/fax interface card with battery reversal detection and Caller ID support (for Europe) [enhanced version of the VIC-2FXO-EU]
VIC-2FXO-M3	Two-port FXO voice/fax interface card for Australia
VIC-2E/M	Two-port E&M voice/fax interface card for voice/fax network module
VIC-2BRI-NT/TE	Two-port network Side ISDN BRI interface
VIC-4FXS/DID[1]	Four-port FXS and DID voice/fax interface card
VWIC-1MFT-T1	One-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1	Two-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1-DI	Two-port RJ-48 multiflex trunk - T1 with drop and insert
VWIC-1MFT-E1	One-port RJ-48 multiflex trunk - E1
VWIC-2MFT-E1	Two-port RJ-48 multiflex trunk - E1

Table 6 Voice Interface Cards for the Cisco 1751

VWIC-2MFT-E1-DI	Two-port RJ-48 multiflex trunk - E1 with drop and insert
VWIC-1MFT-G703	One-port RJ-48 multiflex trunk - E1 G.703
VWIC-2MFT-G703	Two-port RJ-48 multiflex trunk - E1 G.703

[1] The Cisco 1751 can support three VIC-4FXS/DID cards with a maximum of four ports in DID mode

Voice Implementation Requirements

The Cisco 1751 Modular Access Router supports FXO, FXS, E&M, ISDN BRI VICs, and T1/E1 multiflex V/WICs.

The FXO interface allows an analog connection to the central office of the Public Switched Telephone Network

(PSTN). The FXS interface connects basic telephone service phones (home phones), fax machines, key sets, and PBXs through ring voltage and dial tone. The E&M interface allows connection for PBX trunk lines (tie lines). The ISDN-BRI NT/TE VIC is used to connect to the PSTN or a PBX/KTS, whereas the T1/E1 multiflex V/WIC (multiflex V/WIC) supports both data and voice services. The multiservice-ready Cisco 1751-V router version includes all the features needed for immediate integration of data and voice services:

- One DSP—(PVDM-256K-4)
- 32-MB Flash memory
- 64-MB DRAM
- Cisco IOS IP/VOX Plus feature set

VICs and WICs are available separately.

The Cisco 1751 and Cisco 1751-V routers have two DSP module slots on the motherboard and a maximum of eight DSPs are supported per router.

DSP Requirements

Cisco 1751 routers support 3 types of DSP images: high complexity (HC), medium complexity (MC) and Flexi-6. HC and MC are used for analog[1] and BRI (VIC-2BRI-NT/TE) VICs; Flexi-6 is used for T1/E1 VWICs[2] and BRI VIC. MC is introduced in Cisco 1751 starting from Cisco IOS 12.2(8)YN release, which will merge into 12.3(1)T. Therefore, please make sure to use Cisco 12.2(8) YN or later releases when using MC. In addition, starting from 12.2(8)YN release, the default DSP image for BRI VIC is changed from HC to Flexi-6. Table 7 lists the default images for each type of VICs; Table 8 lists IOS support for each DSP image. Table 9 lists the number of channels supported by one DSP (PVDM-256K-4) for each codec type.

Please use the following rules for calculating DSP requirements on the Cisco 1751:

1. For the Early Deployment (ED) releases: Cisco IOS 12.2(2)XK, 12.2(4)XW, 12.2(4)XL, 12.2(4)XM, 12.2(4)YA, 12.2(4)YB, 12.2(8)YL, 12.2(8)YM and 12.2(11)YT, or T train releases prior to 12.3(1)T:

[1] Analog VICs include VIC-2FXS, VIC-2FXO, VIC-2FXO-M1, VIC-2FXO-M2, VIC-2FXO-M3, VIC-2FXO-EU, VIC-2E/M, VIC-2DID,VIC-4FXS/DID

[2] T1/E1 VWICs include VWIC-1MFT-T1, VWIC-2MFT-T1, VWIC-2MFT-T1-DI, VWIC-1MFT-E1, VWIC-2MFT-E1, VWIC-2MFT-E1-DI, VWIC-1MFT-G703, VWIC-2MFT-G703

- a. Each 2-port analog VIC requires 1 DSP (PVDM-256K-4)
- b. Each VIC-2BRI-NT/TE requires 2 DSPs (PVDM-256K-8)
- c. For VWICs, refer to Table 9. For example, 12 G.711 digital T1/E1 voice calls require two DSPs; 12 G.729 calls require four DSPs
- d. Total DSP requirement is the sum of a, b and c. The DSP resources can not be shared between analog VICs, BRI VIC and VWICs.

2. For the Early Deployment (ED) releases: Cisco IOS 12.2(8)YN or later (Note: not including 12.2(11)YT) or T train releases 12.3(1)T or later, please always refer to the DSP Calculator in the following link:

   http://www.cisco.com/cgi-bin/Support/DSP/cisco_prodsel.pl

The DSP calculator optimizes the DSP resources for your configuration and suggests CLI configurations.

Table 7 DSP Firmware for each type of VICs

VIC Type	Firmware Support
2-port Analog VICs	HC (default), MC (starting from 12.2(8)YN)
4-port Analog VIC	HC, MC (default, starting from 12.2(8)YN)
VIC-2BRI-NT/TE	HC (default for ED releases prior to 12.2(8)YN or T train releases prior to 12.3(1)T); MC; Flexi-6 (default for ED releases 12.2(8)YN or later or T train releases 12.3(1)T or later);
T1/E1 VWICs	Flexi-6 (default)

Table 8 Cisco IOS support for DSP firmware

Firmware Support	IOS Release Support
HC	In all orderable IOS Releases
MC	ED Releases: Cisco IOS 12.2(8)YN or later [1] T Train Releases: Cisco IOS 12.3(1)T or later
Flexi-6	For T1/E1 VWICs: • ED Releases: Cisco IOS 12.2(4)YB or later [2] • T Train Releases: 6th releases of 12.2T or later For VIC-2BRI-NT/TE: • ED Releases: Cisco IOS 12.2(8)YN or later [3] • T Train Releases: Cisco IOS 12.3(1)T or later

[1] It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support MC.
[2] It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support Flexi-6.
[3] It doesn't include Cisco 12.2(11)YT. 12.2(11)YT doesn't support Flexi-6.

Table 9 The number of channels supported by one DSP (PVDM-256K-4) per codec type

	Firmware		
Codec	HC (for analog & BRI VICs)	MC (for analog & BRI VICs)	Flexi 6 (for VWICs & BRI VIC[1])

Table 9 The number of channels supported by one DSP (PVDM-256K-4) per codec type

		Firmware	
G.711	2	4	6
G.729ab[2] /G.729a	2	4	3
G.726	2	4	3
G.723	2	-	2
G.728	2	-	2
Fax Relay	2	4	3

[1] BRI VIC support in Flexi-6 starts from 12.2(8)YN or 12.3(1)T.

[2] G.729 and G.729b is not supported in MC or Flexi-6 images.

Table 10 DSP Modules Available on Cisco 1751

Modules	DSPs
PVDM-256K-4	1 DSP Module
PVDM-256K-8	2 DSP Modules
PVDM-256K-12	3 DSP Modules
PVDM-256K-16HD	4 DSP Modules
PVDM-256K-20HD	5 DSP Modules

Cisco IOS Software Feature Sets

The Cisco 1751 Router supports a choice of Cisco IOS Software feature sets. Each feature set requires specific amounts of Flash and DRAM memory in the product. For default memory configurations, please see Table 11.

Table 11 Cisco 1751 Router Memory Defaults and Maximums

Model Number	Default FLASH/Maximum FLASH	Default DRAM/Maximum DRAM
Cisco 1751	16 MB/16 MB	32 MB/96 MB
Cisco 1751-V Multiservice Model	32 MB/32 MB	64 MB/128 MB

The Cisco 1751 Router supports a choice of Cisco IOS Software feature sets with rich data features as well as data/ voice features (Table 12). Each feature set requires specific amounts of RAM and Flash memory in the product.

- Cisco IOS IP base feature sets include: NAT, OSPF, RADIUS, and NHRP.
- Plus feature sets contain L2TP, L2F, the Border Gateway Protocol (BGP), IP Muliticast, Frame Relay SVC, RSVP, the NetWare Link Services Protocol (NLSP), AppleTalk SMRP, the Web Cache Control Protocol (WCCP), and the Network Timing Protocol (NTP).

- Encryption is offered in special encryption feature sets (Plus IPSec 56, and Plus IPSec 3DES). The VPN encryption module requires an IOS IP Plus IPSec image.
- DSL support is only in the Plus feature sets.

Table 12 Cisco IOS Features

Cisco 1751 Router Data Software Feature Sets for Cisco IOS Release 12.1.(5)YB		
Feature Name	**Product Code**	**CD Number**
IP	S17C-12105YB	CD17-C-12.1.5=
IP ADSL	S17C7-12105YB	CD17-C-12.1.5=
IP Plus ADSL	S17C7P-12105YB	CD17-C7P-12.1.5=
IP Plus IPSec 56 (DES) ADSL	S17C7L-12105YB	CD17-C7L-12.1.5=
IP Plus IPSec 3DES ADSL	S17C7K2-12105YB	CD17-C7K2-12.1.5=
IP/FW/IDS	S17CH-12105YB	CD17-CH-12.1.5=
IP/FW/IDS Plus IPSec 56 (DES) ADSL	S17C7HL-12105YB	CD17-C7HL-12.1.5=
IP/IPX	S17B-12105YB	CD17-B-12.1.5=
IP/IPX/FW/IDS Plus ADSL	S17B7HP-12105YB	CD17-B7HP-12.1.5=
IP/FW/IDS Plus IPSec 3DES ADSL	S17C7HK2-12105YB	CD17-C7HK2-12.1.5=
IP/IPX/AT/IBM	S17Q-12105YB	CD17-Q-12.1.5=
IP/IPX/AT/IBM Plus ADSL	S17Q7P-12105YB	CD17-Q7P-12.1.5=
IP/IPX/AT/IBM/FW/IDS Plus IPSec 56 (DES) ADSL	S17Q7HL-12105YB	CD17-Q7HL-12.1.5=
IP/IPX/AT/IBM/FW/IDS Plus IPSec 3DES ADSL	S17Q7HK2-12105YB	CD17-Q7HK2-12.1.5=
Cisco 1751 Router Data/Voice Software Feature Packs for Cisco IOS Release 12.1.(5)YB		
Feature Name	**Product Code**	**CD Number**
IP/Voice Plus	S17CVP-12105YB	CD17-C7VP-12.1.5=
IP/Voice Plus ADSL	S17C7VP-12105YB	CD17-C7VP-12.1.5=
IP/Voice Plus IPSec 56 (DES) ADSL	S17C7VL-12105YB	CD17-C7VL-12.1.5=
IP/Voice/FW/IDS Plus ADSL	S17C7HV-12105YB	CD17-C7HV-12.1.5=
IP/Voice/FW/IDS Plus IPSec 56 ADSL	S17C7HVL-12105YB	CD17-C7HVL-12.1.5
IP/Voice Plus IPSec 3DES ADSL	S17C7VK2-12105YB	CD17-C7VK2-12.1.5=
IP/Voice/FW/IDS Plus IPSec 3DES ADSL	S17C7HVK2-12105YB	CD17-C7HVK2-12.1.5=
IP/IPX/Voice/FW/IDS Plus ADSL	S17B7HPV-12105YB	CD17-B7HPV-12.1.5=
IP/IPX/AT/IBM/FW/IDS Voice Plus IPSec 56 (DES) ADSL	S17Q7HVL-12105YB	CD17-Q7HVL-12.1.5=
IP/IPX/AT/IBM/FW/IDS/Voice Plus IPSec 3DES ADSL	S17Q7HVK2-12105YB	CD17-Q7HVK2-12.1.5=

Other IOS Features Include:

QoS Features

- Frame Relay Fragmentation (FRF.12)
- IP Precedence
- Generic Traffic Shaping (GTS)
- Frame Relay Traffic Shaping (FRTS)
- Weighted Random Early Detection (WRED)
- DSCP Marking
- Compressed RTP
- Multiple Link PPP & Link Fragmentation and Interleaving
- Resourse Reservation Protocol (RSVP)
- Queuing Techniques: Weighted Fair Queuing (WFQ), Priority Queuing (PQ), Low Laterey Queuing (LLQ) and Custom Queuing (CQ)
- Preclassification for IPSec Tunneling

Voice Support

- VoIP
- VoFR
- VoATM
- Fax Pass Through
- Fax Relay
- Modem Pass Through

VoIP Protocol Support

- H.323 V2
- Media Gateway Control Protocol 1.0
- Session Initiation Protocol 2.0

Codec Support

- G.711
- G.729
- G.729a
- G.723.1
- G.726
- G.728

Technical Specifications

Dimensions

- Width: 11.2 in. (28.4 cm)
- Height: 4.0 in. (10.0 cm)
- Depth: 8.7 in. (22.1 cm)
- Weight (minimum): 3.0 lb (1.36 kg)
- Weight (maximum): 3.5 lb (1.59 kg)

Power

- Locking connector on power socket
- External Power Brick
- AC Input Voltage: 100 to 240 VAC
- Frequency: 50 - 60 Hz
- AC Input Current: rated 1 A, measured 0.5 A
- Power Dissipation: 20W (maximum)

Environmental

- Operating Temperature: 32 to 104 F (0 to 40 C)
- Nonoperating Temperature: –4 to 149 F (–20 to 65 C)
- Relative Humidity: 10 to 85% noncondensing operating; 5 to 95% noncondensing, nonoperating

Safety

- Regulatory Approvals
  - UL 1950, 3rd Edition
  - CSA 22.2 No 950-95, 3rd Edition
  - EN60950 with A1 through A4 and A11
  - EN41003
  - TCA TS001–1997
  - AS/NZS 3260 with A1 through A4
- IEC 60950 with A1 through A4 and all country deviations
- NOM-019-SCFI
- GB4943
  - ETSI 300-047
  - BS 6301 (power supply) EMI
  - AS/NRZ 3548 Class B
- CNS-13438
  - FCC Part 15 Class B
  - EN60555-2 Class B

- EN55022 Class B
- VCCI Class II
- CISPR-22 Class B

- EN55024 comprised of:
  - IEC 1000-4-2 (EN61000-4-2)
  - IEC 1000-4-3 (ENV50140)
  - IEC 1000-4-4 (EN61000-4-4)
  - IEC 1000-4-5 (EN61000-4-5)
  - IEC 1000-4-6 (ENV50141)
  - IEC 1000-4-11
  - IEC 1000-3-2 Network Homologation
  -
- Europe: CTR2, CTR3, TBR21
- Canada: CS-03
- United States: FCC Part 68
- Japan: Jate NTT
- Australia/New Zealand: TS013/TS-031, TS002, TS003
- Hong Kong: CR22

Service and Support

Leading-edge technology deserves leading-edge support. Service and support for the Cisco 1751 is available on a one-time or an annual contract basis. Support options range from help desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access to Cisco.com for technical assistance, electronic commerce, and product information
- 24-hour-a-day access to the industry's largest dedicated technical support staff

A support contract maximizes the value of your technology investment throughout its lifecycle, ensuring optimum performance and availability. Augment your internal staff's capabilities by taking full advantage of Cisco expertise.

Contact your local sales office for further information.

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

AP GC

Cisco Confidential

Table of Contents

Q & A

Cisco 1751 Modular Access Router

Product Features and Positioning

What is the ideal environment for the Cisco 1751 router?

A. The Cisco 1751 modular access router is an ideal access solution for small- and medium-sized businesses and small branch offices. The Cisco 1751 is a modular access platform that offers customers secure Internet and intranet access, as well as the capability to implement a variety of applications in the same platform, including voice over IP, virtual-private- network (VPN) access, and business-class Digital Subscriber Line (DSL) access when needed.

In addition to the various functions available on the 1720, the Cisco 1751 provides multiservice integrated voice/data support. By implementing the Cisco 1751 into existing data networks, customers can save on long-distance interoffice phone/fax toll charges while enabling next-generation voice-enabled applications such as integrated messaging and Web based call centers.

The Cisco 1751 router is particularly suitable for environments that require:

- Modularity, flexibility, and investment protection to upgrade to new services and technologies such as multiservice, VPN, and broadband access now or later
- VPN deployment either now or in the future, with requirements for encryption speeds up to T1/E1 (the Cisco 1751

can encrypt at 512 Kbps using software-based encryption, and at T1/E1 using the VPN hardware-based encryption card inserted on the motherboard)

- Multiservice data/voice/fax integration
- Digital voice support (ISDN NT/TE VIC support, VIC-BRI-NT/TE)
- 10/100 Ethernet LAN
- Dual Ethernet capability (with 10BaseT Ethernet WIC)
- VLAN support (802.1Q))
- The flexibility of one voice and two WAN/voice interface card slots
- Higher number of serial interfaces (up to five, including AUX port)
- Dual ISDN Basic Rate Interface (BRI) connections
- Compression at speeds greater than 128 Kbps
- Support for ADSL and G.SHDSL interface card

Q. What are the key differences between the Cisco 1751 and the Cisco 1751-V?

A. The Cisco 1751 and 1751-V support the same data and voice functionality. The main difference between these two models is that the Cisco 1751-V is voice ready, i.e. it comes with higher default memory, 1 DSP module and the IOS IP/Voice PLUS image. Table 1 compares the Cisco 1751 and Cisco 1751-V.

Table 1: Feature Comparison of the Cisco 1751 and the Cisco 1751-V

Cisco 1751	**Cisco 1751-V**
Base version	**Multiservice-ready version**
Includes everything for data networking	Includes all the features needed for *immediate* integration of voice and data
16-MB Flash memory (Non-upgradeable)	32-MB Flash memory (Non-Upgradeable)
32-MB DRAM (on board)	64-MB DRAM (32 MB on board, 32 MB in DRAM DIMM[1] socket)
Cisco IOS IP Software Feature Set	Cisco IOS IP/Voice Plus feature set
Two DSP[2] module slots available DSPs available separately	Two DSP module slots available Comes with one DSP (PVDM-256K-4) inserted in one DSP module slot DSPs available separately for further upgrades
VICs available separately	VICs available separately

Flash memory and DRAM upgrades available separately	Flash memory and DRAM upgrades available separately
WICs available separately	WICs available separately

[1] Double in-line memory module

[2] Digital signal processor

Table 2: Feature Comparison of the Cisco 1751 and Cisco 1750

Feature	Cisco 1751	Cisco 1750
Digital voice support (ISDN BRI VIC and T1/E1 VWICs)	Yes	No
VLAN (IEEE 802.1Q)	Yes	No
Routing performance (64-byte packets)—fast-switching	12,000 pps	8,500 pps
Base models: flash/ DRAM (default)	Cisco 1751: 16/32 Cisco 1751-V: 32/64	Cisco 1750: 4/16 Cisco 1750-2V: 8/32 Cisco 1750-4V: 8/32
No. of PVDM slots	2	1

Q. Is the Cisco 1751 a replacement for the Cisco 1750?

A. The Cisco 1751 is a superior solution when compared to the Cisco 1750 in terms of performance, value and functionality (see Table 2).

Q. Will the Cisco 1750 be discontinued (i.e. EOS)?

A. Yes. Cisco 1750 Router will be end of sale on May 31st 2002. Please refer to the following product bulletin for details: http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/1660_pp.htm

We urge the customers to migrate to the Cisco 1751 due to the clear advantages that it offers at the same price point. The Cisco 1751 Router provides all of the features of the 1750 plus support for; digital voice, VLAN, and greater performance. In addition, the Cisco 1751 Router comes with more memory than the 1750 (both flash and DRAM), which reduces the overall solution cost when deploying voice and/or security features.

Q. What are the differences between the Cisco 1600-R series and the Cisco 1700 series router?

A. Compared with the Cisco 1600-R series, the Cisco 1700 series offers increased performance, added flexibility with fully modular chasses, and investment protection with support for new services such as DSL, Voice over IP (VoIP), and VPNs at similar price points to the Cisco 1600-R. Wherever possible, Cisco encourages customers to move to the new Cisco 1700 platform to be best positioned for future growth and services. Some services (DSL, VoIP) are and will not be supported on the Cisco 1600-R series because of performance and architecture limitations. Table 3 clarifies the features of the Cisco 1600-R and 1700 series families. The Cisco 1600-R series will continue to be available, but Cisco is actively marketing the 1700 series as the next-generation access platform ideal for small- and medium-sized businesses and small branch offices. Most Cisco 1600-R models have a list price of $1495 (US), and an equivalent configuration of the Cisco

1720 is $1595 (US list). For $100, customers get the added benefits of increased performance and the ability to benefit from a broad array of services including VPNs, VoIP, and DSL when needed.

- Secure Internet/intranet access with firewall- and software-based DES and 3DES encryption
- VPN (with optional hardware-based encryption card)
- Multiservice voice with VoIP and Voice over Frame Relay (VoFR)
- ADSL and G.SHDSL
- High-speed LAN (10/100 Ethernet)
- More modularity

Table 3: Key Enhanced Capabilities of Cisco 1751 Series Compared to Cisco 1600-R Series

Feature	Cisco 1600-R Series Modular Access Routers	Cisco 1751 Series Modular Access Routers
WAN slots	1601-R-1604-R: One fixed WAN port plus one modular WAN interface card (WIC) slot 1605-R: One modular WAN interface card (WIC) slot and two 10 Mbps Ethernet ports	Two WAN interface card slots
WAN Interface Cards Supported	Single serial (sync, async): WIC-1T Single ISDN BRI S/T: WIC-1B-S/T Single ISDN BRI U: WIC-1B-U Single serial with integrated 56/64 K DSU: WIC-1DSU-56K4 Single serial with integrated T1/FT1 DSU: WIC-1DSU-T1	All Cisco 1600-R series WAN interface cards plus: Dual serial (sync): WIC-2T Dual serial (async/sync): WIC-2A/S Ethernet WIC: WIC-1ENET ADSL WIC: WIC-1ADSL G.SHDSL WIC: WIC-1SHDSL Modem WIC: WIC-1AM and WIC-2AM
Maximum WAN Interfaces Supported	Two serial (synchronous/asynchronous)	Five serial (sync/async, including the auxiliary port)
	One ISDN BRI (maximum)	Two ISDN BRI
LAN	1601-R-1604-R: One 10BaseT Ethernet port 1605-R: Two 10BaseT Ethernet ports	One autosensing 10/100 Fast Ethernet
Dual Ethernet support	1605-R: Two 10BaseT Ethernet ports	One autosensing 10/100 Fast

		Ethernet on-board interface + 10BaseT Ethernet WIC
VLAN support (802.1Q)	No	Yes
Support for Voice Interface Cards (VICs)	No	Yes: 2-port ear and mouth (E&M) voice interface card (VIC) 2-port Direct Inward Dial (DID) 2-port Foreign Exchange Office (FXO) VIC, and 2-port Foreign Exchange Station (FXS) VIC 2-port Network/Userside BRI (VIC-2BRI-NT/TE) 1 or 2-port T1/E1 Multiflex VWICs
Maximum Voice Channels Supported	None	Analog: 6 total (2 slots support voice or WAN interface cards; all voice cards provide 2 voice ports) Digital: 24 total (T1/E1 Multiflex VWICs)
AUX Port (async up to 115.2 kbps)	No	Yes
Support for Dual ISDN BRI	No	Yes
Encryption Support	DES	DES, triple DES
IPSec DES Encryption Speed	Software performance (DES, 256-byte packets) 128 Kbps (ISDN)	Software performance (3DES, 256-byte packets) 256 Kbps (2xISDN) Performance with VPN module (3DES, 256-byte packets) 1700 Kbps (T1/E1)
Expansion Slot for High-Speed Hardware-Based Encryption	No	Yes

Card		
Maximum Flash Memory	16 MB	Cisco1751: 16MB Cisco1751-V: 32MB
Maximum DRAM Memory	24 MB	Cisco1751: 96 MB Cisco1751-V: 128MB

Q. Will the Cisco 1600-R support DSL or VPN or multiservice voice or 10/100 Ethernet or 3DES encryption in the future?

A. No. The Cisco 1600-R series was not designed to support the above technologies.

Q. Should we position Cisco 1700 series to the customer instead of 1600-R?

A. Yes. Always. Please educate the value proposition of the Cisco 1700 series and the applications and services that it can support either now or later. We strongly suggest the sales team to help educate the customer to invest in Cisco 1700 series and avoid the cost of upgrading later.

Q. What is the proper positioning of the Cisco 1700 series, and 2600 series routers?

A. The Cisco 1700 series routers are positioned for small- and medium-sized businesses and small branch offices. Because of its modularity, increased performance, and investment protection capabilities, the Cisco 1700 is a strategic platform for small- and medium-sized businesses and small branch offices. The Cisco 2600 series routers are positioned as enterprise-class solutions for enterprise large branch offices, offering rack-mount for wiring-closet environments, internal power supply, and optional redundant power supply. The Cisco 2600 series offers a flexible, modular solution with higher performance; more WAN density such as dual ISDN Primary Rate Interface (PRI), 10 ISDN BRIs, four T1/E1s, 36 async serial interfaces; and support for dial and digital voice with densities ranging from two to 60 calls.

These four router families are positioned as two winning pairs:

- Cisco 1700 series for small and medium-sized businesses and enterprise small branch offices
- Cisco 2600 series for enterprise branch offices

Q. When would a customer want a Cisco 2600 series router rather than a Cisco 1751 router?

A. The Cisco 2600 series is better suited for larger enterprise branch offices that require multiple WAN ports and, typically, a 19-inch rack-mount enclosure. It provides two WAN interface card slots, plus an additional network module slot, which provides higher port densities as well as support for voice services. The key differences are highlighted in Table 4.

Table 4: Key Differences between Cisco 1751 Router and Cisco 2600 Series Routers

Feature	**Cisco 1751**	**Cisco 2600 Series**
Performance (fast-switch 64-byte packets)	12,000 pps	12,000 to 37,000 pps

Performance (IPSec DES-encrypted 256-byte Packets)	512 Kbps	512 Kbps
"Class of Product"	Small/medium business and small enterprise branch office	"Enterprise class"
	Desktop	19-in. rack-mount, ideal for wiring closets
	External power supply	Internal power supply
	No redundant power supply option	Redundant power supply option
	Optional Plus feature sets for enterprise-class software features (IP multicast, RSVP, BGP, and so on)	Enterprise-class software features standard in Base IP, for example, IP multicast, RSVP, BGP
	No enterprise or APPN feature sets	Enterprise and APPN feature sets
	Not NEBS compliant	NEBS compliant
	No Token Ring LAN	Token Ring LAN option
Support for Voice Interface Cards	Yes: supports dual port E&M, FXO, FXS, DID and ISDN BRI NT/TE, T1/E1 Multiflex VWICs	Yes: supports dual-port E&M, FXO, FXS, ISDN BRI-N/T-TE and BRI-ST/TE, digital T1/E-1 packet voice trunk network module, T1/E-1 multiflex WAN/voice interface card (multiflex WAN/voice interface card)
Maximum Voice Interfaces Supported	Analog: 4 ports with 1 WAN slot (up to dual T1/E1 WIC) or 6 ports without WAN access Digital: 24 calls with one channelized T1 or E1 or 12 ports without WAN access	2 to 60 voice calls
Maximum WAN Densities	4 serial, 2 BRI, 4 A/S	10 BRI, 12 A/S, 36 A, 2 PRI, 1 ATM
Maximum LAN Density	2 (one on-board 10/100 and an optional Ethernet WIC)	6 Ethernet
Slots	2 WAN/voice interface cards + 1 voice interface card	2 WAN interface cards + 1 network module
	1 internal expansion slot for VPN hardware encryption card	1 AIM slot for encryption, compression, voice processing, ATM SAR

Voice	Voice-over-IP (VoIP), VoFR	Voice/fax-over-IP capable, VoFR capable
Integrated Dial Capability	Not supported	16 modem or 32 async serial

Q. Which Cisco IOS® release is available with the Cisco 1751 at first customer ship (FCS)?

A. At FCS, the Cisco 1751 router shipped with Cisco IOS Release 12.1(5)YB, which is a special release. The Cisco 1751 router will be available on the 12.2T Release train in 12.2(4)T.

Software Feature Sets

Q. What software feature sets are available for the Cisco 1751 router?

A. Twenty-four feature sets are available (see Table 5). This includes 14 data images and 10 data and voice images.

Table 5: Minimum Memory Requirements and Software Feature Sets for Cisco IOS Releases 12.1(5)YB

Cisco IOS Feature Set	**Memory Requirement**	
	FLASH	**DRAM**
IP	4MB	24MB
IP/ADSL	8MB	24MB
IP/ADSL Plus	8MB	32MB
IP/ADSL Plus IPSec 56	8MB	32MB
IP/FW/IDS	4MB	24MB
IP/ADSL/FW/IDS Plus IPSec 56	8MB	32MB
IP/IPX	4MB	24MB
IP/ADSL/IPX/FW/IDS Plus	8MB	32MB
IP/ADSL Plus IPSec 3DES	8MB	32MB
IP/ADSL/FW/IDS Plus IPSec 3DES	8MB	32MB
IP/IPX/AT/IBM	8MB	24MB
IP/ADSL/IPX/AT/IBM Plus	16MB	48MB
IP/ADSL/IPX/AT/IBM/FW/IDS Plus IPSec 56	16MB	48MB

IP/ADSL/IPX/AT/IBM/FW/IDS Plus IPSec 3DES	16MB	48MB
IP/ADSL/VoicePlus	8MB	32MB
IP/Voice Plus	8MB	32MB
IP/ADSL/Voice Plus IPSec 56	16MB	48MB
IP/ADSL/FW/IDS/VoicePlus	16MB	48MB
IP/ADSL/FW/IDS/Voice Plus IPSec 56	16MB	48MB
IP/IPX/FW/IDS/Voice Plus	16MB	48MB
IP/ADSL Voice Plus IPSec 3DES	16MB	48MB
IP/ADSL/FW/IDS/Voice Plus IPSec 3DES	8MB	32MB
IP/ADSL/IPX/AT/IBM/FW/IDS/VoicePlus IPSec 56	16MB	48MB
IP/ADSL/IPX/AT/IBM/FW/IDS/Voice Plus IPSec 3DES	16MB	48MB

Check on Cisco Release Notes for the recent software feature sets and minimum memory requirements. http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122relnt/index.htm

Starting with Cisco IOS Release 12.0, the base feature sets on the 1600/1700 series include some features formerly in the PLUS feature sets: Network Address Translation (NAT), Open Shortest Path First (OSPF), Remote Access Dial-In User Service (RADIUS), and Next Hop Resolution Protocol (NHRP). Plus feature sets contain all the features in their corresponding Base feature sets, plus additional value-added features such as Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F), Border Gateway Protocol (BGP), IP multicast, Frame Relay, Switched Virtual Circuit (SVC), Resource Reservation Protocol (RSVP), PPPoE, NetWare Link Services Protocol (NLSP), AppleTalk Simple Multicast Routing Protocol (SMRP), and Network Timing Protocol (NTP).

Tables 6 through 8 show the features available in the Cisco IOS 1751 feature sets.

Table 6: Features in Cisco IOS Base Feature Sets

Category	Basic Protocols/Features	IP	IP/ADSL	IP/IPX	IP Firewall	IP/IPX/AT/IBM
LAN	Transparent bridging	X	X	X	X	X
	IP	X	X	X	X	X
	IPX, NetBIOS access lists, name caching			X		X
	AppleTalk phases 1 and 2					X

WAN	Leased lines, Frame Relay, Switched 56, SMDS, HDLC	X	X	X	X	X
	ISDN leased line (IDSL) at 64 and 128 Kbps	X	X	X	X	X
	ISDN Caller ID callback	X	X	X	X	X
	PPP, PPP compression	X	X	X	X	X
	Async, SLIP	X	X	X	X	X
	X.25, X.25 PAD, X.25 over ISDN D channel	X	X	X	X	X
	LLC2, LAPB	X	X	X	X	X
IP Routing	RIP, RIP2, IGRP, Enhanced IGRP, OSPF, NHRP	X	X	X	X	X
	IP policy routing	X	X	X	X	X
	GRE tunneling	X	X	X	X	X
Other Routing	IPX-RIP			X		X
	(AppleTalk) RTMP					X
Security	PAP/CHAP, local password	X	X	X	X	X
	Extended access lists; Lock and Key	X	X	X	X	X
	RADIUS, TACACS+, Token Ring	X	X	X	X	X
Quality of Service (QoS)	Weighted Fair Queueing (WFQ)	X	X	X	X	X
WAN Optimization	Bandwidth on demand, dial on demand	X	X	X	X	X
	IPX and SPX spoofing			X		X
	Snapshot routing	X	X	X	X	X
	Frame Relay FRF.9	X	X	X	X	X
Ease of Use and						

Deployment	ConfigMaker	X	X	X	X	X
	Easy IP (PAT, IPCP, and DHCP server)	X	X	X	X	X
	Network Address Translation (NAT)	X	X	X	X	X
	AutoInstall for leased line and Frame Relay	X	X	X	X	X
Management	SNMP, Telnet, console port	X	X	X	X	X
	CiscoView, CiscoWorks2000	X	X	X	X	X
	Simple Network Timing Protocol (SNTP)	X	X	X	X	X

Note: AppleTalk routing and bridging are not supported for asynchronous interfaces.

Table 7: Data Only Plus Feature Sets—Additional Features

Category	Plus Protocols/ Features	IP/ADSL Plus	IP/ADSL Plus IPSec 56	IP/ADSL Plus IPSec 3DES	IP/ADSL FW/IDS Plus IPSec 56	IP/ADSL FW/IDS Plus IPSec 3DES	IP/ADSL/IPX FW/IDS Plus
WAN	Frame Relay SVC	X	X	X	X	X	X
IP Routing	BGP	X	X	X	X	X	X
Other Routing	NetWare Link Services Protocol						X
	AppleTalk AURP, ATIP						
VPN/Security	IPSec DES		X	X	X	X	
	IPSec Triple DES			X		X	
VPN/Tunnels	L2TP, L2F	X	X	X	X	X	X

QoS	Resource Reservation Protocol (RSVP)	X	X	X	X	X	X
	Random Early Detection (RED)	X	X	X	X	X	X
	Cisco Express Forwarding (CEF)	X	X	X	X	X	X
	Committed access rate (CAR)	X	X	X	X	X	X
	NetFlow	X	X	X	X	X	X
	RTP Header Compression (RTP-HC)	X	X	X	X	X	X
Multi media	IP Multicast (Protocol Independent Multicast, or PIM)	X	X	X	X	X	X
	AppleTalk SMRP (multicast)						
Management	Network Timing Protocol (NTP)	X	X	X	X	X	X

Note: FW denotes Cisco IOS Firewall Feature Set. Encryption is offered in special encryption feature sets (Plus IPSec 56 and Plus IPSec 3DES). To build an IP VPN, the recommended images are IP Firewall Plus IPSec 56 or IP Firewall Plus IPSec 3DES.

Table 8: Data and Voice Plus Feature Sets—Additional Features

Category	**Plus Protocol/Features**	**IP/ADSL/Voice Plus**	**IP/ADSL/FW/IDS/ Voice Plus**	**IP/ADSL/Voice Plus IPSec 56**	**IP/ADSL/V Plus IPSec 3DES**
WAN	Frame Relay SVC	X	X	X	X

IP Routing	BGP	X	X	X	
Other Routing	NetWare Link Services Protocol				
	AppleTalk AURP, ATIP				
VPN/Security	IPSec DES			X	X
	IPSec Triple DES				X
VPN/Tunnels	L2TP, L2F	X	X	X	X
QoS	Resource Reservation Protocol (RSVP)	X	X	X	X
	Random Early Detection (RED)	X	X	X	X
	Cisco Express Forwarding (CEF)	X	X	X	X
	Committed Access Rate (CAR)	X	X	X	X
	NetFlow	X	X	X	X
	RTP Header Compression (RTP-HC)	X	X	X	X
Multi media	IP Multicast (Protocol Independent Multicast, or PIM)	X	X	X	X
	AppleTalk SMRP (multicast)				
Codes	G.711	X	X	X	X
	G.729a	X	X	X	X
	G.723.1	X	X	X	X
	G.726	X	X	X	X

Voice Features	Voice over IP	X	X	X	X
	Fax support (group III fax)	X	X	X	X
	Private Line Automatic Ringdown (PLAR)	X	X	X	X
	Support for Off-premise Extension (OPX)	X	X	X	X
	Support for FXS	X	X	X	X
	Support for FXO	X	X	X	X
	Support for E&M	X	X	X	X
	Support for ISDN NT/TE VIC	X	X	X	X
	Voice Activity Detection (VAD)	X	X	X	X
	Busy out	X	X	X	X
	Comfort noise generation	X	X	X	X
	H.323 Version 1 and 2	X	X	X	X
	DTMF relay	X	X	X	X
	FRF.12	X	X	X	X
QoS	MLPPP w/ LFI (process-switched)	X	X	X	X
	FRF traffic shaping with per VC queuing	X	X	X	X
	IP RTP priority	X	X	X	X
	cRTP (Fast-switched)	X	X	X	X

MLPPP w/ LFI (fast-switched)	X	X	X	X
LLQ (PQ/CBWFQ)	X	X	X	X
FRF.11 (VoFR)	X	X	X	X
DiffServ	X	X	X	X

LAN Functionality

Q. What types of LANs does the Cisco 1751 router support?

A. The Cisco 1751 router supports one autosensing 10/100 Fast Ethernet connection, with one 10/100BaseTX ransceiver (RJ-45 connector). The 10/100BaseTX port can connect to an external 10/100BaseTX hub or switch or ectly to a PC Ethernet port (using a crossover cable) using inexpensive, unshielded twisted-pair (UTP) wiring.

Q. Is the 10BaseT Ethernet WIC supported on the 1751?

A. Yes, the 10Base T Ethernet WIC is supported on the 1751 to provide dual Ethernet functionality.

Q. What LAN and routing protocols are supported by the Cisco 1751 router?

A. The Cisco 1751 router supports IP, Internetwork Packet Exchange (IPX), AppleTalk routing, IBM Systems Network Architecture (SNA), and transparent bridging. Routing protocols supported include IP Routing Information Protocol (RIP), RIP V.2, Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), IPX-RIP, OSPF, on-demand OSPF, NHRP, and AppleTalk Routing Table Maintenance Protocol (RTMP). Additionally, Plus feature sets including: BGP, NLSP and AppleTalk Update-Based Routing Protocol (AURP) are supported in Plus feature sets that support IPX and AppleTalk, respectively.

Q. Is it possible to manually set the Fast Ethernet (FE) speed on the Cisco 1751?

A. Yes, this feature was implemented in releases 12.1 and 12.1T. With prior releases, the FE port speed is tonegotiated.

Q. Is ISL or IEEE802.1Q supported on the Cisco 1751?

A. IEEE802.1Q is supported on the Cisco 1751. ISL is not supported. The Cisco 1720 and 1750 do not support VLAN (IEEE 802.1Q or ISL).

WAN Functionality

Q. What WAN interface cards are available?

A. Available WAN interface cards are shown in Table 9.

Table 9: Available WAN Interface Cards

WAN Interface Card	Interfaces

WIC-1T	1 serial, async and sync (T1/E1)
WIC-2T	2 serial, async and sync (T1/E1)
WIC-2A/S	2 low-speed (up to 128 kbps) serial, async, and sync
WIC-1B-S/T	1 ISDN BRI S/T
WIC-1B-U	1 ISDN BRI U with integrated NT1
WIC-1DSU-56K4	1 integrated 56/64 Kbps 4-wire DSU/CSU
WIC-1DSU-T1	1 integrated T1/fractional T1 DSU/CSU
WIC-1ENET	1 10BaseT Ethernet (only supported in Slot 0)
WIC-1ADSL	1 ADSL
WIC-1SHDSL	1 G.SHDSL
WIC-1AM	1 V.90 modem card
WIC-2AM	2 V.90 modem card

Q. Are there any WIC slot dependencies with respect to order or maximum number of a certain type?

A. All WICs are supported in any slot and in any combination.

Q. Does the Cisco 1751 router support two ISDN BRI interfaces?

A. Yes. The Cisco 1751 router supports two BRI interfaces (dial and ISDN leased line) with two ISDN BRI WAN interface cards installed in the two WAN interface card slots. Multilink PPP (MP) can combine the four B channels to achieve data rates up to 256 Kbps.

Q. Do the WIC-1T, WIC-2T, and WIC-2A/S WAN interface cards support asynchronous serial when installed in the Cisco 1751 router?

A. Yes. The Cisco 1751 router supports asynchronous serial (up to 115.2 Kbps) as well as synchronous serial on the serial WAN interface cards. The onboard aux port also supports asynchronous serial at speeds up to 115.2 Kbps.

Q. What WAN protocols does the Cisco 1751 router support?

A. Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), X.25 Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), Frame Relay, and IBM/SNA are supported over permanent or switched digital lines. PPP and Serial Line Internet Protocol (SLIP) are supported over asynchronous analog lines.

Q. Do the serial ports on the Cisco 1751 router support data-communications-equipment (DCE) functionality?

A. Yes, the Cisco 1751 router supports DCE (that is, supplies clocking), allowing the Cisco 1751 router to interconnect without requiring a null modem. Also, X.25 packet assembler/disassembler (PAD) functionality is supported. IBM Synchronous Data Link Control (SDLC), bisync, and other serial protocols are supported.

Q. Is IDSL supported on the Cisco 1751?

A. No.

Q. Will the Cisco 1751 support three WICs?

A. The Cisco 1751 can only support two WAN interfaces. The AUX port can be used as another WAN port. If your customer needs greater density, the Cisco 2600 would be the solution.

Q. Does the Cisco 1751 Router support Modem WIC card?

A. Yes. The Cisco 1751 Router supports one and two-port V.90 modem WIC card. Product number is WIC-1AM and WIC-2AM. For more details about the Modem WIC, please refer to the following data sheet:

http://www.cisco.com/warp/public/cc/pd/rt/1700/prodlit/17srt_ds.htm

Voice Functionality

Q. Does Cisco 1751 support Survivable Remote Site Telephony (SRST)?

Yes. For the detailed information, please refer to the below documents

Announcement: http://www.cisco.com/cpropart/salestools/cc/pd/rt/1700/prodlit/1601_po.htm

Datasheet: http://www.cisco.com/warp/partner/synchronicd/cc/pd/unco/srstl/prodlit/srstd_ds.htm

Q. What voice interface cards (VICs) are supported on the Cisco 1751?

A. The voice interface cards currently supported are given in Table 10.

Table 10: Voice Interface Cards Currently Supported

Voice Interface Card	**Interfaces**
VIC-2DID	2-port direct inward dial (DID) voice/fax interface card
VIC-2E/M	2-port voice interface card E&M
VIC-2FXO	2-port voice interface card FXO
VIC-2FXS	2-port voice interface card FXS
VIC-2FXO-M1	2-port FXO voice/fax interface card with battery reversal detection and Caller ID support (for U.S. and Canada) [enhanced version of the VIC-2FXO]
VIC-2FXO-M2	2-port FXO voice/fax interface card with battery reversal detection and Caller ID support (for Europe) [enhanced version of the VIC-2FXO-EU]
VIC-2FXO-M3	2-port voice interface card FXO (for Australia)
VIC-2FXO-EU	2-port voice interface card FXO (for Europe)

VIC-2BRI-NT/TE	2-port network side/terminal side ISDN BRI interface
VWIC-1MFT-T1	1-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1	2-port RJ-48 multiflex trunk - T1
VWIC-2MFT-T1-DI	2-port RJ-48 multiflex trunk - T1 with drop and insert
VWIC-1MFT-E1	1-port RJ-48 multiflex trunk - E1
VWIC-2MFT-E1	2-port RJ-48 multiflex trunk - E1
VWIC-2MFT-E1-DI	2-port RJ-48 multiflex trunk - E1 with drop and insert
VWIC-1MFT-G703	1-port RJ-48 multiflex trunk - E1 G.703
VWIC-2MFT-G703	2-port RJ-48 multiflex trunk - E1 G.703

Q. How many DSPs are supported in the 1751?

A. The 1751 has 2 DSP module slots on the motherboard, each of which supports the 5 DSP module. This provides a DSP density of 10 DPS's.

Q. What are the PVDM/VIC combinations that are supported?

A. The supported combinations are shown in Table 11.

Table 11: Supported PVDM/VIC Combinations

PVDM	**Number of DSPs Supported**	**VIC Combinations**
PVDM- 256K-4	1	1 analog VIC
PVDM-256K-8	2	Up to 2 analog VICs or 1 voice-BRI VIC
PVDM-256K-12	3	Up to 3 analog VICs or 1 analog VIC + 1 voice-BRI VIC

PVDM-256K-16	4	Up to 3 analog VICs or Up to 2 voice-BRI VICs or Up to 2 analog VICs+1 voice-BRIVIC
PVDM-256K-20	5	Up to 3 analog VICs or Up to 2 voice-BRI VICs or Upto 2 analog VICs+1 voice- BRIVIC or 1 analog VIC+up to 2 voice-BRI VICs

Q. Are the PVDM-4 (supported in Cisco 1750) supported in Cisco 1751?

A. PVDM-4, 8,12 are not officially supported in the Cisco1751.

Q. Are the PVDM-256K-4 (supported in Cisco 1751) supported in Cisco 1750?

A. PVDM-256K-4, 8,12 are not officially supported in the Cisco1751.

Q. Does the 1751 support digital VICs?

A. Yes, the 1751 supports digital VICs. At FCS, the ISDN BRI NT/TE VIC is supported, and 1 or 2 port T1/E1 VWICs are supported in Cisco IOS 12.2(4)YB or later releases.

Q. Does the Cisco 1751 support the T1/E1 VWICs (i.e. the multi-flex cards)?

A. Yes. From Cisco IOS 12.2(4) YB or later releases. It will roll into 5th 12.2 T train release.

Q. How many DSPs are required to support the various VICs?

Q. The analog VICs require 1 DSP/VIC, the ISDN BRI VIC requires 2 DSPs/VIC. For T1/E1 VWICs, it depends on the codec and how many voice channels are used. The number of maximum channels support per DSP is listed in Table 12.

Table 12: Maximum Channels Support per DSP for T1/E1 Multiflex VWICs

Codec	**Kbps**	**Max Channels/DSP** **(Digital Calls)**
G.711	64 (PCM)	6
G.729a	8 (CS-ACELP)	3
G.726	16 (ADPCM)	3
G.723.1	5.3/6.3 (ACELP)	2
G.728	32 (ADPCM/LDCLP)	2

For example, if you are running 12 G.711 digital T1/E1 voice calls, then you will need two DSPs. If these are G.729 calls, then you will need four DSPs.

DSP used for the digital calls and for the analog calls have to be calculated separately and one DSP can support multiple Codecs concurrently for T1/E1 VWICs.

487e

Q. Does Cisco 1751 support Caller ID?

A. Yes, Cisco 1751 supports Caller ID transmission on FXS, FXO-M1 and FXO-M2 interfaces. It provides Caller ID blocking configurable at the source location on FXS, and ability to unblock Caller ID on FXO-M1, M2 interfaces.

Q. Does Cisco 1751 support analog DID trunk card?

A. Yes.

Q. What does toll reduction or toll bypass mean?

A. In most of today's corporate networks, voice networks are separate from data networks. Typically, data networks are priced by a monthly fixed cost basis and are usually much cheaper than the voice networks. An example of this is a leased-line environment. In this case, the customer pays for that network, whether data is flowing or not. In a typical phone network, charges are incurred on a usage basis. Therefore, phone expenses on interoffice dialing can be quite expensive, especially since most interoffice calling occurs during "peak" business hours.

When you have the ability to put your interoffice voice calls across a lower-price or fixed-price network with a product such as the Cisco 1751 platform, you can avoid the "toll" that is charged by the long-distance carrier, local exchange carrier (LEC), or Port, Telephone, and Telegraph (PTT). The voice call then travels over the same network that your dat travels over and avoids going into the Public Switched Telephone Network (PSTN) and, therefore, does not incur charges.

It is easy for companies to figure out the savings that they will get, because they receive accurate monthly reports that describe their costs from their LECs. Any company that does a great deal of interoffice calling will save more money than one that does more "off-net" PSTN-type calling.

Q. What do the terms FXO, FXS, and E&M mean?

A. The Cisco 1751 router supports FXO, FXS, and E&M voice interface cards. Each type provides a slightly different interface for connecting to different types of equipment.

Foreign Exchange Office

The FXO interface allows an analog connection to be directed at the central office (CO) of the PSTN. This interface is of value for off-premise extension applications. This is the only voice interface card that will be approved to connect to of premise lines. This interface may be used to provide backup over the PSTN or for Centrex-type operations. This voice interface card needs to be approved by PTTs; it is not available in every country. Check the homologation status page at http://wwwin-eng.cisco.com/Eng/MSABU/Eng_Ops/WWW/index.htmfor up-to-date availability information.

Foreign Exchange Station

The FXS interface allows connection for basic telephone service phones (home phones), fax machines, keysets, and private branch exchange (PBXs) by providing ring voltage, dial tone, and so on. This interface will be used where phones are connecting directly to the router. FXS will be very popular for trials because it allows the phones to be plugged directly into the router.

Ear and Mouth

The E&M interface allows connection for PBX trunk lines (tie lines). It is a signaling technique for two- and four-wire telephone and trunk interfaces.

Q. What's the difference between FXO and FXO-M1, FXO-M2?

A. VIC-2FXO-M1 and VIC-2FXO-M2 support battery reversal detection and Caller ID. While the regular VIC-2FXO doesn't. VIC-2FXO-M1 is for U.S. and Canada, VIC-2FXO-M2 is for Europe.

Q. Does the Cisco 1751 support three analog VICs, or six analog voice ports?

A. Yes. Customers requiring this capability need to order the PVDM-256k-12 module (part number: PVDM-256k-12=), which provides three DSPs.

Q. Is RAS for H.323 gatekeeper registration supported on the Cisco 1751 platform?

A. Yes.

Q. In a VoFR and VoIP environment, there are cases where people using OPX extensions would like to use their message waiting lights at the remote sites. To provide functionality, the 150 V signal must be sensed on the originating end and reproduced on the terminating side. Is the message waiting function supported on the Cisco 1751?

The FXS port does not have the ability to provide the voltage levels necessary to perform this function.

Q. What are the key features when implementing voice on the Cisco 1751?

A. Please refer to Cisco 1700 Modular Access Voice Feature Overview

http://wwwin.cisco.com/cmc/cc/pd/rt/1700/sales/orwir_st.htm

Cisco IOS Security

Q. What security functions are available for the Cisco 1751 router?

A. Cisco IOS software supports a wide range of security features. Standard features in base feature sets include access control lists (ACLs); authentication, authorization, and accounting (AAA) features such as Password Authentication Protocol/Challenge Handshake Authentication Protocol (PAP/CHAP), TACACS+, RADIUS, and Token Ring; and Lock and Key. Optional features include the Cisco IOS Firewall Feature Set, IP Security (IPSec) encryption, and tunneling protocols such as IPSec, generic routing encapsulation (GRE), L2F, and L2TP.

Q. Can I use the Cisco 1751 router as a firewall?

A. Yes. The Cisco IOS Firewall Feature Set is supported in the Cisco 1751 router. This feature set offers enhanced firewall functionality, including context-based access control (CBAC), which enables securing a network on a per-application basis. Additional firewall security features include Java applet blocking, denial-of-service detection and prevention, and more advanced logging capabilities. For more information, see: http://www.cisco.com/warp/partner/synchronicd/cc/cisco/mkt/security/iosfw/index.htmpartner/synchronicd/cc/cisco/mkt

Q. Can I encrypt data on the Cisco 1751 router?

A. Yes. Two types of encryption technologies are supported: IPSec Data Encryption Standard (DES) 56 and IPSec Triple DES.

Processor

Q. What is the processor on the Cisco 1751 router?

A. The Cisco 1751 router uses a Motorola MPC860P PowerQUICC at 48 MHz. The Cisco 2600 series uses an MPC860 The 860P processor of the Cisco 1751 router has an integrated Fast Ethernet controller. This has implications on performance, as discussed in the Performance section.

Performance

Q. How does the performance of the Cisco 1700 series compare to that of the Cisco 1600-R series?

A. As Table 13 shows, the Cisco 1751 router performance is greater than that of the Cisco 1600-R series.

Table 13: Performance Comparison of the Cisco 1600-R Series and the Cisco 1751

Feature	**Cisco 1600-R Series**	**Cisco 1751**
Encryption IPSec DES 56 (256-byte packets)	128 Kbps	512 Kbps
Encryption IPSec 3DES (256-byte packets)	Not supported	256 Kbps
Fast Switching (64-byte packets)	2 Mbps (4000 pps)	4.3 Mbps (8400 pps)
Processor Switching (64-byte packets)	300 Kbps (600 pps)	768 Kbps (1500 pps)

Q. How does the performance of the Cisco 1751 router compare with that of the Cisco 2600 series routers?

A. The Cisco 2600 series router has higher fast-switching performance (12,000 to 37,000 pps for 64-byte packets) compared to the Cisco 1751 router (8400 pps). However, the encryption and process switching performance for both platforms are similar (512 Kbps for IPSec DES 56 encryption with 256 byte packets; 768 Kbps or 1500 pps for process switching of 64-byte packets).

Q. Why is the fast-switching performance of the Cisco 1751 router not equal to that of the Cisco 2600 series when they appear to use the same processor?

A. The Cisco 1751 router uses a Motorola MPC860P processor, which is different from the MPC860 processor on the Cisco 2600 series. The Motorola 860P has an integrated Fast Ethernet controller. This processor uses an arbitration scheme that continuously polls for contenders for the Fast Ethernet bus in a round-robin fashion. Contenders are the serial communications controllers (SCCs), Ethernet controller, and cache. This process of round-robin polling uses up clock cycles, resulting in lower fast-switching performance.

Internal Expansion Slot and Encryption Card

Q. Can the internal expansion slot of the Cisco 1751 router support the advanced integration module (AIM) expansion cards (for example, encryption) that is supported on the Cisco 2600 series?

A. No. The Cisco 2600 series has an AIM slot that is based on a protocol control information (PCI)-bus architecture; th Cisco 1751 router, on the other hand, uses a Q-bus to lower cost. Although the expansion cards on these platforms are not the same, the encryption technology is interoperable and, therefore, creates a complete Cisco end-to-end solution.

Q. Does the Cisco 1751 support the 1700 VPN module that accelerates DES and 3DES for IPSec?

A. Yes. See VPN Module Q&A at:
http://wwwin.cisco.com/Mkt/cmc/cc/cisco/mkt/access/1700/internal/vpn17_qa.htmvpn17_qa.htm.

Compression

Q. Does the Cisco 1751 router support compression?

A. Yes. Up to 4:1 compression is supported. The Cisco 1751 router supports both Stac and predictor compression algorithms. Compression performance for the Cisco 1751 router has not been measured yet.

Q. What compression algorithms are supported on the Cisco 1751 router?

A. The WAN interfaces of the Cisco 1751 router support the types of compression algorithms for each of the WAN encapsulations given in Table 14.

Table 14: Compression Algorithms Supported on the Cisco 1751 Router

Encapsulation	Compression Algorithm
PPP	Predictor stacker
Frame Relay	Payload
HDLC	Stac
X.25	Payload
LAPB	Predictor Stac

IBM/SNA Features

Q. What IBM/SNA features are available for Cisco 1751 router?

A. The supported IBM/SNA features on the Cisco 1751 router are equivalent to those supported on the Cisco 1600-R, 2500, and 2600 series routers (see Table 15):

Table 15: IBM/SNA Features Supported on the Cisco 1751 Router

STUN	**NetBIOS**
SDLC	SNA priority queue
SDLLC	NetView NSP
Bisync	BSTUN native client interface architecture (NCIA) server
DLSW+ (data-link switching plus)	Local acknowledgment
QLLC	RSRB (required for DLSw)
FRAS (BNN, BAN, RFC 1490)	Response time reporter (internetwork performance monitor)
IBM Network Manager/LAN Manager	All CiscoWorks Blue (maps and so on)

DSPU	All Cisco IBM MIBs

Note: Token Ring and Advanced Peer-to-Peer Networking (APPN), supported on the Cisco 2500 and 2600 series, are not supported on Cisco 1600-R series and 1751 routers.

Q. Will the Cisco 1751 router support Token Ring interfaces?

A. No, there are no plans to support Token Ring on the Cisco 1751 router.

Q. When do I sell a Cisco 1751 router IBM solution?

A. The Cisco 1751 router is best sold for IBM/SNA opportunities that require:

- One Ethernet/1-5 WAN configuration (including the AUX)
- Modularity/flexibility—The Cisco 1751 series provides two WAN interface card slots, allowing customers to add or change WAN services as needed
- Multiservice voice/data integration now or in the future

Q. What IBM/SNA software feature sets are available for Cisco 1751 router?

A. IBM/SNA feature sets available for Cisco 1751 router include:

- IP/IPX/AppleTalk/IBM
- IP/ADSL/IPX/AppleTalk/IBM Plus
- IP/ADSL/IPX/AT/IBM/FW/IDS Plus IPSec 56
- IP/ADSL/IPX/AT/IBM/FW/IDS Plus IPSec 3DES
- IP/ADSL/IPX/AT/IBM/FW/IDS/Voice Plus IPSec 56
- IP/ADSL/IPX/AT/IBM/FW/IDS/Voice Plus IPSec 3DES

Note Use Plus for L2F, L2TP, BGP, NTP, NLSP, RSVP, IP multicast, Frame Relay SVC, and encryption support.

Memory Architecture

Q. What memory architecture does the Cisco 1751 router use?

Q. The Cisco 1751 router uses the run-from-RAM memory architecture.

Q. What type of DRAM memory does the Cisco 1751 router use?

A. The Cisco 1751 router uses synchronous DRAM (SDRAM). The default DRAM is 32 MB fixed onboard for the 1751 model, and 64 MB for the 1751-V model. There is one DIMM slot for adding additional memory in increments of 16, 32, and 64 MB. The maximum DRAM for the 1751 model is 96MB (32 MB onboard plus 64 MB DIMM). The maximum DRAM for the 1751-V model is 128MB (64 MB onboard plus 64 MB DIMM).

	Cisco 1751	Cisco 1751-V
Default DRAM (MB)	32	64
Max. DRAM (MB)	96	128

Q. What type of Flash memory does the Cisco 1751 router use?

A. The Cisco 1751 router uses onboard (soldered on the motherboard) flash. The Cisco1751 has 16 MB of flash. The Cisco 1751-V have 32 MB of flash. This is a fixed configuration—it is not upgradeable and there is not a flash card slot on the motherboard to add more flash.

	Cisco 1751	Cisco 1751-V
Default Flash (MB)	16	32
Max. Flash (MB)	16	32

Q. What is the flash memory used for?

A. Cisco IOS software and configuration files are stored flash. Also, flash memory allows software upgrades to be downloaded over the WAN or LAN link to be stored in the Mini-Flash card.

Q. How are software images and configuration files stored in flash?

A. Flash come preprogrammed with Cisco IOS software. Software upgrades and configuration files must be copied using Trivial File Transfer Protocol (TFTP) onto a Mini-Flash card in a Cisco 1751 router.

Q. Is dual Flash bank supported on Cisco 1751 routers?

A. Yes. Dual Flash bank is supported. Although both the Cisco 1751 and Cisco 1751-V support dual flash bank, we recommend that customers requiring dual flash bank purchase the Cisco 1751-V model since it comes with 32 MB flash.

Q. Does the Cisco 1751 use the same DRAM as the Cisco 1720/1750?

A. Yes. However, the Cisco 1751 does not support the 4 and 8 MB DIMM (MEM1700-4D= and MEM1700-8D=). In addition there is a new 64MB DIMM available for the Cisco 1751

Q. Does the Cisco 1751 use the same flash as the Cisco 1720/1750?

A. No. The flash in the Cisco 1751 is soldered on the motherboard, and is therefore not upgradeable.

Q. Can the amount of shared (input/output [I/O]) memory on a Cisco 1751 router be configured?

A. Yes. It can be modified using Cisco IOS command-line interface (CLI) and saved as part of the router configuration.

Power Supply

Q. What type of power supplies does the Cisco 1751 router use?

A. The Cisco 1751 router uses one universal power supply that is applicable for all countries. There are no country-specific power supplies. The AC input voltage of this universal power supply spans from 100 to 240 V; the frequency from 47 to 64 Hz. (Although this power supply works in all countries, the user still has to specify the power cord appropriate for a particular country.) The router also has a locking connector on the power socket to ensure that the power cord remains securely fastened.

MTBF

Q. What is the mean time between failures (MTBF) for the Cisco 1751 router?

A. The predicted MTBF is 514,526 hours. This predicted MTBF includes the chassis and external power supply but not the WAN interface cards or voice interface cards.

Network Management

Q. How is the Cisco 1751 router managed?

A. Like all Cisco routers, the Cisco 1751 router can be managed via Simple Network Management Protocol (SNMP), via a Telnet session, and through a directly connected terminal or PC running terminal emulator software.

Q. Do CiscoView, CiscoWorks2000, and Cisco Voice Manager support Cisco 1751 routers?

A. Yes, CiscoView, CiscoWorks2000 and Cisco Voice Manager supported.

Q. Does Cisco ConfigMaker support Cisco 1751 routers?

A. Yes, Cisco ConfigMaker supports Cisco 1751 routers, starting with Release 2.5b.

Q. Does the Cisco 1751 router support Remote Monitoring (RMON)?

A. The Cisco 1751 router supports only RMON lite. RMON lite covers two out of the nine RMON groups, alarms, and events. Full RMON (statistics, history, hosts, hostTopN, matrix, filter, capture) features are available for the Cisco 2500 and 2600 series routers.

HOME CONTENTS PREVIOUS NEXT PDF SEARCH HELP

Posted: Wed Aug 21 23:43:46 PDT 2002

AP G D

Cisco IOS File System Commands

This chapter describes the basic set of commands used to manipulate files on your routing device using the Cisco IOS File System (IFS) in Cisco IOS Release 12.2.

Commands in this chapter use URLs as part of the command syntax. URLs used in the Cisco IFS contain two parts: a file system or network prefix, and a file identification suffix. The following tables list URL keywords that can be used in the *source-url* and *destination-url* arguments for all commands in this chapter. The prefixes listed below can also be used in the *filesystem* arguments in this chapter.

Table 18 lists common URL network prefixes used to indicate a device on the network.

Table 18 Network Prefixes for Cisco IFS URLs

Prefix	Description
ftp:	Specifies a File Transfer Protocol (FTP) network server.
rcp:	Specifies an remote copy protocol (rcp) network server.
tftp:	Specifies a TFTP server.

Table 19 lists the available suffix options (file indentification suffixes) for the URL prefixes used in Table 18.

Table 19 File ID Suffixes for Cisco IFS URLs

Prefix	Suffix Options
ftp:	[[//[username[:password]@]location]/directory]/filename For example: **ftp://network-config** (*prefix://filename*) **ftp://jeanluc:secret@enterprise.cisco.com/ship-config**
rcp:	rcp:[[//[username@]location]/directory]/filename
tftp:	tftp:[[//location]/directory]/filename

Table 20 lists common URL prefixes used to indicate memory locations on the system.

Table 20 File System Prefixes for Cisco IFS URLs

Prefix	Description
bootflash:	Bootflash memory.
disk0:	Rotating disk media.
flash: [*partition-number*]	Flash memory. This prefix is available on most platforms. For platforms that do not have a device named **flash:**, the prefix **flash:** is aliased to **slot0:**. Therefore, you can use the prefix **flash:** to refer to the main Flash memory storage area on all platforms
flh:	Flash load helper log files.
null:	Null destination for copies. You can copy a remote file to null to determine its size.
nvram:	NVRAM. This is the default location for the running-configuration file.
slavebootflash:	Internal Flash memory on a slave RSP card of a router configured with Dual RSPs.
slavenvram:	NVRAM on a slave RSP card.
slaveslot0:	First PCMCIA card on a slave RSP card.
slaveslot1:	Second PCMCIA card on a slave RSP card.
slot0:	First PCMCIA Flash memory card.
slot1:	Second PCMCIA Flash memory card.
xmodem:	Obtain the file from a network machine using the Xmodem protocol.
ymodem:	Obtain the file from a network machine using the Ymodem protocol.

For details about the Cisco IFS, and for IFS configuration tasks, refer to the "Configuring the Cisco IOS File System" chapter in the Release 12.2 *Cisco IOS Configuration Fundamentals Configuration Guide*.

cd

To change the default directory or file system, use the **cd** EXEC command.

cd [*filesystem*:]

Syntax Description

filesystem:	(Optional) The URL or alias of the directory or file systems followed by a colon.

Defaults

The initial default file system is **flash:**. For platforms that do not have a physical device named **flash:**, the keyword **flash:** is aliased to the default Flash device.

If you do not specify a directory on a file system, the default is the root directory on that file system.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

For all EXEC commands that have an optional *filesystem* argument, the system uses the file system specified by the **cd** command when you omit the optional *filesystem* argument. For example, the **dir** EXEC command, which displays a list of files on a file system, contain an optional *filesystem* argument. When you omit this argument, the system lists the files on the file system specified by the **cd** command.

Examples

In the following example, the cd command is used to set the default file system to the Flash memory card inserted in slot 0:

```
Router# pwd
bootflash:/
Router# cd slot0:
Router# pwd
slot0:/
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the **cd** command.
show file systems	Lists available file systems and their alias prefix names.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

configure network

The **configure network** command was replaced by the **copy** {**rcp** | **tftp**} **running-config** command in Cisco IOS Release 11.0. To maintain backward compatibility, the **configure network** command continues to function in Cisco IOS Release 12.2 for most systems, but support for this command may be removed in a future release.

The **copy** {**rcp** | **tftp**} **running-config** command was replaced by the **copy** {**ftp:** | **rcp:** | **tftp:**}[*filename*] **system:running-config** command in Cisco IOS Release 12.1.

The **copy** {**ftp:** | **rcp:** | **tftp:**}[*filename*] **system:running-config** command specifies that a configuration file should be copied from a FTP, rcp, or TFTP source to the running configuration. See the description of the **copy** in this chapter command for more information.

copy

To copy any file from a source to a destination, use the **copy** EXEC command.

copy [**/erase**] *source-url destination-url*

Syntax Description

/erase	(Optional) Erases the destination file system before copying.
source-url	The location URL or alias of the source file or directory to be copied.
destination-url	The destination URL or alias of the copied file or directory.

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or an alias keyword for a file system type (not a file within a type).

Timesaver Aliases are used to cut down on the amount of typing you need to perform. For example, it is easier to type **copy run start** (the abbreviated form of the **copy running-config startup-config** command) than it is to type **copy system:r nvram:s** (the abbreviated form of the **copy system:running-config nvram:startup-config** command). These aliases also allow you to continue using some of the common commands used in previous versions of Cisco IOS software.

Table 21 shows two keyword shortcuts to URLs.

Table 21 Common Keyword Aliases to URLs

Keyword	Source or Destination
running-config	(Optional) Keyword alias for the **system:running-config** URL. The **system:running-config** keyword represents the current running configuration file. This keyword does not work in **more** and **show file** EXEC command syntaxes.
startup-config	(Optional) Keyword alias for the **nvram:startup-config** URL. The **nvram:startup-config** keyword represents the configuration file used during initialization (startup). This file is contained in NVRAM for all platforms except the Cisco 7000 family, which uses the CONFIG_FILE environment variable to specify the startup configuration. The Cisco 4500 series cannot use the **copy running-config startup-config** command. This keyword does not work in **more** and **show file** EXEC command syntaxes.

The following tables list aliases by file system type. If you do not specify an alias, the router looks for a file in the current directory.

Table 22 lists URL aliases for Special (opaque) file systems. Table 23 lists them for network file systems, and Table 24 lists them for local writable storage.

Table 22 URL Prefix Aliases for Special File Systems

Alias	Source or Destination
flh:	Source URL for flash load helper log files.
modem:	Destination URL for loading modem firmware on Cisco 5200 and 5300 Series routers.
nvram:	Router NVRAM. You can copy the startup configuration into or from NVRAM. You can also display the size of a private configuration file.
null:	Null destination for copies or files. You can copy a remote file to null to determine its size.
system:	Source or destination URL for system memory, which includes the running configuration.
xmodem:	Source destination for the file from a network machine that uses the Xmodem protocol.
ymodem:	Source destination for the file from a network machine that uses th Xmodem protocol.

Table 23 URL Prefix Aliases for Network File Systems

Alias	Source or Destination
ftp:	Source or destination URL for an File Transfer Protocol (FTP) network server. The syntax for this alias is as follows: **ftp:**[[[//*username* [:*password*]@]*location*]/*directory*]/*filename*.
rcp:	Source or destination URL for a Remote Copy Protocol (rcp) network server. The syntax for this alias is as follows: **rcp:**[[[//*username*@]*location*]/*directory*]/*filename*.
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is **tftp:**[[//*location*]/*directory*]/*filename*.

Table 24 URL Prefix Aliases for Local Writable Storage File Systems

Alias	Source or Destination
bootflash:	Source or destination URL for boot flash memory.
disk0: and disk1:	Source or destination URL of rotating media.
flash:	Source or destination URL for Flash memory. This alias is available on all platforms. For platforms that lack a flash: device, note that **flash:** is aliased to **slot0:**, allowing you to refer to the main Flash memory storage area on all platforms.
slavebootflash:	Source or destination URL for internal Flash memory on the slave RSP card of a router configured for HSA.
slaveram:	NVRAM on a slave RSP card of a router configured for HSA.
slaveslot0:	Source or destination URL of the first PCMCIA card on a slave RSP card of a router configured for HSA.

Table 24 URL Prefix Aliases for Local Writable Storage File Systems (continued)

Alias	Source or Destination
slaveslot1:	Source or destination URL of the second PCMCIA slot on a slave RSP card of a router configured for HSA.
slot0:	Source or destination URL of the first PCMCIA Flash memory card.
slot1:	Source or destination URL of the second PCMCIA Flash memory card.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

You can enter on the command line all necessary source- and destination-URL information and the username and password to use, or you can enter the **copy** command and have the router prompt you for any missing information.

If you enter information, choose one of the following three options: **running-config**, **startup-config**, or a file system alias (see previous tables.) The location of a file system dictates the format of the source or destination URL.

The colon is required after the alias. However, earlier commands not requiring a colon remain supported, but are unavailable in context-sensitive help.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

In the alias syntax for **ftp:**, **rcp:**, and **tftp:**, the location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers.

This section contains usage guidelines for the following topics:

- Understanding Invalid Combinations of Source and Destination
- Understanding Character Descriptions
- Understanding Partitions
- Using rcp
- Using FTP
- Storing Images on Servers
- Copying from a Server to Flash Memory
- Verifying Images
- Copying a Configuration File from a Server to the Running Configuration
- Copying a Configuration File from a Server to the Startup Configuration
- Storing the Running or Startup Configuration on a Server
- Saving the Running Configuration to the Startup Configuration

- Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables
- Using the Copy Command with the Dual RSP Feature

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, you cannot copy the following:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

Understanding Character Descriptions

Table 25 describes the characters that you may see during processing of the **copy** command.

Table 25 copy Character Descriptions

Character	Description
!	For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each).
.	For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.
O	For network transfers, an uppercase O indicates that a packet was received out of order and the copy process may fail.
e	For Flash erasures, a lowercase e indicates that a device is being erased.
E	An uppercase E indicates an error. The copy process may fail.
V	A series of uppercase Vs indicates the progress during the verification of the image checksum.

Understanding Partitions

You cannot copy an image or configuration file to a Flash partition from which you are currently running. For example, if partition 1 is running the current system image, copy the configuration file or image to partition 2. Otherwise, the copy operation will fail.

You can identify the available Flash partitions by entering the **show file system** EXEC command.

Using rcp

The rcp protocol requires a client to send a remote username upon each rcp request to a server. When you copy a configuration file or image between the router and a server using rcp, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The remote username specified in the **copy** command, if a username is specified.
2. The username set by the **ip rcmd remote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the router software sends the Telnet username as the remote username.
4. The router host name.

For the rcp copy request to process, an account must be defined on the network server for the remote username. If the network administrator of the destination server did not establish an account for the remote username, this command will not run. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

If you are writing to the server, the rcp server must be properly configured to accept the rcp write request from the user on the router. For UNIX systems, add an entry to the .rhosts file for the remote user on the rcp server. Suppose the router contains the following configuration lines:

```
hostname Rtr1
ip rcmd remote-username User0
```

If the router IP address translates to Router1.company.com, then the .rhosts file for User0 on the rcp server should contain the following line:

```
Router1.company.com Rtr1
```

Refer to the documentation for your rcp server for more details.

If you are using a personal computer as a file server, the computer must support the remote shell protocol (rsh).

Using FTP

The FTP protocol requires a client to send a remote username and password upon each FTP request to a server. When you copy a configuration file from the router to a server using FTP, the Cisco IOS software sends the first valid username that it encounters in the following sequence:

1. The username specified in the **copy** command, if a username is specified.
2. The username set by the **ip ftp username** command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the **copy** command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.
3. The router forms a password username@routername.domain. The variable username is the username associated with the current session, routername is the configured host name, and domain is the domain of the router.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the router.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

Refer to the documentation for your FTP server for more details.

Use the **ip ftp username** and **ip ftp password** global configuration commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify a username for that copy operation only.

Storing Images on Servers

Use the **copy** *flash: destination-url* command (for example, **copy flash: tftp:**) to copy a system image or boot image from Flash memory to a network server. Use the copy of the image as a backup copy. Also, use it to verify that the copy in Flash memory is the same as that in the original file.

Copying from a Server to Flash Memory

Use the **copy** *destination-url flash:* command (for example, **copy tftp: flash:**) to copy an image from a server to Flash memory.

On Class B file system platforms, the system provides an option to erase existing Flash memory before writing onto it.

Note Verify the image in Flash memory before booting the image.

Verifying Images

When copying a new image to your router, you should confirm that the image was not corrupted during the copy process. Depending on the destination filesystem type, a checksum for the image file may be displayed when the **copy** command completes. You can verify this checksum by comparing it to the checksum value provided for your image file on Cisco.com.

Caution If the checksum values do not match, do not reboot the router. Instead, reissue the **copy** command and compare the checksums again. If the checksum is repeatedly wrong, copy the original image back into Flash memory *before* you reboot the router from Flash memory. If you have a corrupted image in Flash memory and try to boot from Flash memory, the router will start the system image contained in ROM (assuming booting from a network server is not configured). If ROM does not contain a fully functional system image, the router might not function and will need to be reconfigured through a direct console port connection.

An alternate method for file verification is to use the UNIX 'diff' command. This method can also be applied to file types other than Cisco IOS images. If you suspect that a file is corrupted, copy the suspect file and the original file to a Unix server. (The file names may need to be modified if you try to save the files in the same directory.) Then run the Unix 'diff' command on the two files. If there is no difference, then the file has not been corrupted.

Copying a Configuration File from a Server to the Running Configuration

Use the **copy** {**ftp:** | **rcp:** | **tftp:**} **running-config** command to load a configuration file from a network server to the running configuration of the router (note that **running-config** is the alias for the **system:running-config** keyword). The configuration will be added to the running configuration as if the commands were typed in the command-line interface (CLI). Thus, the resulting configuration file will be a combination of the previous running configuration and the loaded configuration file, with the loaded configuration file having precedence.

You can copy either a host configuration file or a network configuration file. Accept the default value of *host* to copy and load a host configuration file containing commands that apply to one network server in particular. Enter *network* to copy and load a network configuration file containing commands that apply to all network servers on a network.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy** {**ftp:** | **rcp:** | **tftp:**} **nvram:startup-config** command to copy a configuration file from a network server to the router startup configuration. These commands replace the startup configuration file with the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy system:running-config** {**ftp:** | **rcp:** | **tftp:**} command to copy the current configuration file to a network server using FTP, rcp, or TFTP. Use the **copy nvram:startup-config** {**ftp:** | **rcp:** | **tftp:**} command to copy the startup configuration file to a network server.

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the **copy system:running-config nvram:startup-config** command to copy the running configuration to the startup configuration.

Note Some specific commands might not get saved to NVRAM. You will need to enter these commands again if you reboot the machine. These commands are noted in the documentation. We recommend that you keep a listing of these settings so you can quickly reconfigure your router after rebooting.

If you issue the **copy system:running-config nvram:startup-config** command from a bootstrap system image, a warning will instruct you to indicate whether you want your previous NVRAM configuration to be overwritten and configuration commands to be lost. This warning does not appear if NVRAM contains an invalid configuration or if the previous configuration in NVRAM was generated by a bootstrap system image.

On all platforms except Class A file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to NVRAM.

On the Class A Flash file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to the location specified by the CONFIG_FILE environment variable. This variable specifies the device and configuration file used for initialization. When the CONFIG_FILE environment variable points to NVRAM or when this variable does not exist (such as at first-time startup), the software writes the current configuration to NVRAM. If the current configuration is too large for NVRAM, the software displays a message and stops executing the command.

When the CONFIG_FILE environment variable specifies a valid device other than **nvram:** (that is, **flash:**, **bootflash:**, **slot0:**, or **slot1:**), the software writes the current configuration to the specified device and filename, and stores a distilled version of the configuration in NVRAM. A distilled version is one that does not contain access list information. If NVRAM already contains a copy of a complete configuration, the router prompts you to confirm the copy.

Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables

For the Class A Flash file system platforms, specifications are as follows:

- The CONFIG_FILE environment variable specifies the configuration file used during router initialization.
- The BOOT environment variable specifies a list of bootable images on various devices.
- The BOOT environment variable specifies a list of bootable images on various devices.
- The BOOTLDR environment variable specifies the Flash device and filename containing the rxboot image that ROM uses for booting.

- Cisco 3600 routers do not use a dedicated boot helper image (rxboot), which many other routers use to help with the boot process. Instead, the BOOTLDR ROM monitor environment variable identifies the Flash memory device and filename that are used as the boot helper; the default is the first system image in Flash memory.

To view the contents of environment variables, use the **show bootvar** EXEC command. To modify the CONFIG_FILE environment variable, use the **boot config** global configuration command. To modify the BOOTLDR environment variable, use the **boot bootldr** global configuration command. To modify the BOOT environment variable, use the **boot system** global configuration command. To save your modifications, use the **copy system:running-config nvram:startup-config** command.

When the destination of a **copy** command is specified by the CONFIG_FILE or BOOTLDR environment variable, the router prompts you for confirmation before proceeding with the copy. When the destination is the only valid image in the BOOT environment variable, the router also prompts you for confirmation before proceeding with the copy.

Using the Copy Command with the Dual RSP Feature

The Dual RSP feature allows you to install two Route/Switch Processor (RSP) cards in a single router on the Cisco 7507 and Cisco 7513 platforms.

On a Cisco 7507 or Cisco 7513 router configured for Dual RSPs, if you copy a file to **nvram:startup-configuration** with automatic synchronization disabled, the system asks if you also want to copy the file to the slave startup configuration. The default answer is **yes**. If automatic synchronization is enabled, the system automatically copies the file to the slave startup configuration each time you use a **copy** command with **nvram:startup-configuration** as the destination.

Examples

The following examples illustrate uses of the **copy** command.

- Copying an Image from a Server to Flash Memory Examples
- Saving a Copy of an Image on a Server Examples
- Copying a Configuration File from a Server to the Running Configuration Example
- Copying a Configuration File from a Server to the Startup Configuration Example
- Copying the Running Configuration to a Server Example
- Copying the Startup Configuration to a Server Example
- Saving the Current Running Configuration Example
- Moving Configuration Files to Other Locations Examples
- Copying an Image from the Master RSP Card to the Slave RSP Card Example

Copying an Image from a Server to Flash Memory Examples

The following three examples use a **copy rcp:**, **copy tftp:**, or **copy ftp:** command to copy an image file from a server to Flash memory:

- Copying an Image from a Server to Flash Memory Example
- Copying an Image from a Server to a Flash Memory Using Flash Load Helper Example
- Copying an Image from a Server to a Flash Memory Card Partition Example

Copying an Image from a Server to Flash Memory Example

This example copies a system image named file1 from the remote rcp server with an IP address of 172.16.101.101 to Flash memory. On Class B file system platforms, the Cisco IOS software allows you to first erase the contents of Flash memory to ensure that enough Flash memory is available to accommodate the system image.

```
Router# copy rcp://netadmin@172.16.101.101/file1 flash:file1

Destination file name [file1]?
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101 (via Ethernet0): ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'file1' from server
  as 'file1' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee...erased
Loading file1 from 172.16.101.101 (via Ethernet0): !
[OK - 984/8388608 bytes]

Verifying checksum... OK (0x14B3)
Flash copy took 0:00:01 [hh:mm:ss]
```

Copying an Image from a Server to a Flash Memory Using Flash Load Helper Example

The following example copies a system image into a partition of Flash memory. The system will prompt for a partition number only if there are two or more read/write partitions or one read-only and one read/write partition and dual Flash bank support in boot ROMs. If the partition entered is not valid, the process terminates. You can enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?***number*) for directory display of a particular partition. The default is the first read/write partition. In this case, the partition is read-only and has dual Flash bank support in boot ROM, so the system uses Flash Load Helper.

```
Router# copy tftp: flash:

System flash partition information:
Partition   Size     Used     Free     Bank-Size   State        Copy-Mode
    1       4096K    2048K    2048K    2048K       Read Only    RXBOOT-FLH
    2       4096K    2048K    2048K    2048K       Read/Write   Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]

                             **** NOTICE ****
Flash load helper v1.0
This process will accept the copy options and then terminate
the current system image to use the ROM based image for the copy.
Routing functionality will not be available during that time.
If you are logged in via telnet, this connection will terminate.
Users with console access can see the results of the copy operation.
                             ---- ******** ----
Proceed? [confirm]
System flash directory, partition 1:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [255.255.255.255]? 172.16.1.1
Source file name? master/igs-bfpx-100.4.3
Destination file name [default = source name]?

Loading master/igs-bfpx.100-4.3 from 172.16.1.111: !
```

```
Erase flash device before writing? [confirm]
Flash contains files. Are you sure? [confirm]
Copy 'master/igs-bfpx.100-4.3' from TFTP server
as 'master/igs-bfpx.100-4.3' into Flash WITH erase? [yes/no] yes
```

Copying an Image from a Server to a Flash Memory Card Partition Example

The following example copies the file c3600-i-mz from the rcp server at IP address 172.23.1.129 to the Flash memory card in slot 0 of a Cisco 3600 series router, which has only one partition. As the operation progresses, the Cisco IOS software asks you to erase the files on the Flash memory PC card to accommodate the incoming file. This entire operation takes 18 seconds to perform, as indicated at the end of the example.

```
Router# copy rcp: slot0:

PCMCIA Slot0 flash

Partition   Size    Used      Free      Bank-Size  State          Copy Mode
  1         4096K   3068K     1027K     4096K      Read/Write     Direct
  2         4096K   1671K     2424K     4096K      Read/Write     Direct
  3         4096K      0K     4095K     4096K      Read/Write     Direct
  4         4096K   3825K      270K     4096K      Read/Write     Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]

PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   3142288  c3600-j-mz.test
[3142352 bytes used, 1051952 available, 4194304 total]
Address or name of remote host [172.23.1.129]?
Source file name? /tftpboot/images/c3600-i-mz
Destination file name [/tftpboot/images/c3600-i-mz]?
Accessing file '/tftpboot/images/c3600-i-mz' on 172.23.1.129...
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz: ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy '/tftpboot/images/c3600-i-mz' from server
  as '/tftpboot/images/c3600-i-mz' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying checksum...  OK (0xF89A)
Flash device copy took 00:00:18 [hh:mm:ss]
```

Saving a Copy of an Image on a Server Examples

The following four examples use **copy** commands to copy image files to a server for storage:

- Copy an Image from Flash Memory to an rcp Server Example
- Copy an Image from a Partition of Flash Memory to a Server Example
- Copying an Image from a Flash Memory File System to an FTP Server Example
- Copying an Image from Boot Flash Memory to a TFTP Server Example

Copy an Image from Flash Memory to an rcp Server Example

The following example copies a system image from Flash Memory to an rcp server using the default remote username. Because the rcp server address and filename are not included in the command, the router prompts for it.

```
Router# copy flash: rcp:

IP address of remote host [255.255.255.255]? 172.16.13.110
Name of file to copy? gsxx
writing gsxx - copy complete
```

Copy an Image from a Partition of Flash Memory to a Server Example

The following example copies an image from a particular partition of Flash memory to an rcp server using a remote username of netadmin1.

The system will prompt if there are two or more partitions. If the partition entered is not valid, the process terminates. You have the option to enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?***number*) for a directory display of a particular partition. The default is the first partition.

```
Router# configure terminal
Router# ip rcmd remote-username netadmin1
Router# end
Router# copy flash: rcp:
System flash partition information:
Partition   Size    Used    Free    Bank-Size   State       Copy-Mode
    1       4096K   2048K   2048K   2048K       Read Only   RXBOOT-FLH
    2       4096K   2048K   2048K   2048K       Read/Write  Direct
[Type ?<number> for partition directory; ? for full directory; q to abort]
Which partition? [1] 2

System flash directory, partition 2:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [ABC.CISCO.COM]?
Source file name? master/igs-bfpx.100-4.3
Destination file name [master/igs-bfpx.100-4.3]?
Verifying checksum for 'master/igs-bfpx.100-4.3' (file # 1)... OK
Copy 'master/igs-bfpx.100-4.3' from Flash to server
as 'master/igs-bfpx.100-4.3'? [yes/no] yes
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Copying an Image from a Flash Memory File System to an FTP Server Example

The following example copies the file c3600-i-mz from partition 1 of the Flash memory card in slot 0 to an FTP server at IP address 172.23.1.129.

```
Router# show slot0: partition 1

PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   1711088 c3600-i-mz
[1711152 bytes used, 2483152 available, 4194304 total]

Router# copy slot0:1:c3600-i-mz ftp://myuser:mypass@172.23.1.129/c3600-i-mz
Verifying checksum for '/tftpboot/cisco_rules/c3600-i-mz' (file # 1)...  OK
Copy '/tftpboot/cisco_rules/c3600-i-mz' from Flash to server
  as 'c3700-i-mz'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

Copying an Image from Boot Flash Memory to a TFTP Server Example

The following example copies an image from boot Flash memory to a TFTP server:

```
Router# copy bootflash:file1 tftp://192.168.117.23/file1

Verifying checksum for 'file1' (file # 1)... OK
Copy 'file1' from Flash to server
  as 'file1'? [yes/no]y
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Copying a Configuration File from a Server to the Running Configuration Example

The following example copies and runs a configuration filename host1-confg from the netadmin1 directory on the remote server with an IP address of 172.16.101.101:

```
Router# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config

Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Router#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

Copying a Configuration File from a Server to the Startup Configuration Example

The following example copies a configuration file host2-confg from a remote FTP server to the startup configuration. The IP address is172.16.101.101, the remote username is netadmin1, and the remote password is ftppass.

```
Router# copy ftp://netadmin1:ftppass@172.16.101.101/host2-confg nvram:startup-config
Configure using rtr2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file rtr2-confg:![OK]
[OK]
Router#
%SYS-5-CONFIG_NV:Non-volatile store configured from rtr2-config by
FTP from 172.16.101.101
```

Copying the Running Configuration to a Server Example

The following example specifies a remote username of netadmin1. Then it copies the running configuration file named rtr2-confg to the netadmin1 directory on the remote host with an IP address of 172.16.101.101.

```
Router# configure terminal
Router(config)# ip rcmd remote-username netadmin1
Router(config)# end
Router# copy system:running-config rcp:
Remote host[]? 172.16.101.101

Name of configuration file to write [Rtr2-confg]?
Write file rtr2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
```

Copying the Startup Configuration to a Server Example

The following example copies the startup configuration to a TFTP server:

```
Router# copy nvram:startup-config tftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [rtr2-confg]? <cr>
Write file rtr2-confg on host 172.16.101.101?[confirm] <cr>
![OK]
```

Saving the Current Running Configuration Example

The following example copies the running configuration to the startup configuration. On a Class A Flash file system platform, this command copies the running configuration to the startup configuration specified by the CONFIG_FILE variable.

```
copy system:running-config nvram:startup-config
```

The following example shows the warning that the system provides if you try to save configuration information from bootstrap into the system:

```
Router(boot)# copy system:running-config nvram:startup-config

Warning: Attempting to overwrite an NVRAM configuration written
by a full system image. This bootstrap software does not support
the full configuration command set. If you perform this command now,
some configuration commands may be lost.
Overwrite the previous NVRAM configuration?[confirm]
```

Enter **no** to escape writing the configuration information to memory.

Moving Configuration Files to Other Locations Examples

On some routers, you can store copies of configuration files on a Flash memory device. Five examples follow.

Copying the Startup Configuration to a Flash Memory Device Example

The following example copies the startup configuration file (specified by the CONFIG_FILE environment variable) to a Flash memory card inserted in slot 0:

```
copy nvram:startup-config slot0:router-confg
```

Copying the Running Configuration to a Flash Memory Device Example

The following example copies the running configuration from the router to the Flash memory PC card in slot 0:

```
Router# copy system:running-config slot0:berlin-cfg

Building configuration...
```

```
5267 bytes copied in 0.720 secs
```

Copying to the Running Configuration from a Flash Memory Device Example

The following example copies the file named ios-upgrade-1 from the Flash memory card in slot 0 to the running configuration:

```
Router# copy slot0:4:ios-upgrade-1 system:running-config

Copy 'ios-upgrade-1' from flash device
  as 'running-config' ? [yes/no] yes
```

Copying to the Startup Configuration from a Flash Memory Device Example

The following example copies the router-image file from the Flash memory to the startup configuration:

```
copy flash:router-image nvram:startup-config
```

Copying a Configuration File from one Flash Device to Another Example

The following example copies the file running-config from the first partition in internal Flash memory to the Flash memory PC card in slot 1. The checksum of the file is verified, and its copying time of 30 seconds is displayed.

```
Router# copy flash: slot1:

System flash

Partition    Size     Used      Free      Bank-Size  State          Copy Mode
  1          4096K    3070K     1025K     4096K      Read/Write     Direct
  2         16384K    1671K    14712K     8192K      Read/Write     Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]

System flash directory, partition 1:
File  Length   Name/status
  1   3142748  dirt/images/mars-test/c3600-j-mz.latest
  2   850      running-config
[3143728 bytes used, 1050576 available, 4194304 total]

PCMCIA Slot1 flash directory:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
  2   850      running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config
Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)...  OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'running-config' from flash: device
  as 'running-config' into slot1: device WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
!
 [OK - 850/4194304 bytes]

Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum...  OK (0x16)
```

Copying an Image from the Master RSP Card to the Slave RSP Card Example

The following example copies the router-image file from the Flash memory card inserted in slot 1 of the master RSP card to slot 0 of the slave RSP card in the same router:

```
copy slot1:router-image slaveslot0:
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
boot system	Specifies the system image that the router loads at startup.
cd	Changes the default directory or file system.
copy xmodem: flash:	Copies any file from a source to a destination.
copy ymodem: flash:	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
erase	Erases a file system.
ip rcmd remote-username	Configures the remote username to be used when requesting a remote copy using rcp.
reload	Reloads the operating system.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
show (Flash file system)	Displays the layout and contents of a Flash memory file system.
slave auto-sync config	Turns on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Backup.
verify bootflash:	Either of the identical **verify bootflash:** or **verify bootflash** commands replaces the **copy verify bootflash** command. Refer to the **verify** command for more information.

delete

To delete a file from a Flash memory device or NVRAM, use the **delete** EXEC command.

delete *URL* [**/force** | **/recursive**]

Syntax Description

URL	IFS URL of the file to be deleted. Include the filesystem prefix, followed by a colon, and, optionally, the name of a file or directory.
/force	(Optional) Deletes the specified file or directory with prompting you for verification. **Note** Use this keyword with caution: the system will not ask you to confirm the file deletion.
/recursive	(Optional) Deletes all files in the specified directory, as well as the directory itself.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

If you attempt to delete the configuration file or image specified by the CONFIG_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion.

When you delete a file in Flash memory, the software simply marks the file as deleted, but it does not erase the file. To later recover a "deleted" file in Flash memory, use the **undelete** EXEC command. You can delete and undelete a file up to 15 times.

To permanently delete all files marked "deleted" on a linear Flash memory device, use the **squeeze** EXEC command.

Examples

The following example deletes the file named "test" from the Flash filesystem:

```
Router# delete flash:test
Delete flash:test? [confirm]
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.

Command	Description
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

dir

To display a list of files on a file system, use the **dir** EXEC command.

dir [**/all**] [*filesystem*:][*file-url*]

Syntax Description

/all	(Optional) Lists deleted files, undeleted files, and files with errors.
filesystem:	(Optional) File system or directory containing the files to list, followed by a colon.
file-url	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Defaults

The default file system is specified by the **cd** command. When you omit the **/all** keyword, the Cisco I software displays only undeleted files.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use the **show** (Flash file system) command to display more detail about the files in a particular file system.

Examples

The following is sample output from the **dir** command:

```
Router# dir slot0:

Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  5  -rw-         639   Oct 02 1997 12:09:32 rally
  7  -rw-         639   Oct 02 1997 12:37:13  the_time

20578304 bytes total (3104544 bytes free)

Router# dir /all slot0:

Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  3  -rw-     7982828   Oct 01 1997 18:48:14  [rsp-jsv-mz]
  4  -rw-         639   Oct 02 1997 12:09:17  [the_time]
```

```
5   -rw-          639    Oct 02 1997 12:09:32  rally
6   -rw-          639    Oct 02 1997 12:37:01  [the_time]
7   -rw-          639    Oct 02 1997 12:37:13  the_time
```

Table 26 describes the significant fields shown in the displays.

Table 26 dir Field Descriptions

Field	Description
1	Index number of the file.
-rw-	Permissions. The file can be any or all of the following: • d—directory • r—readable • w—writable • x—executable
4720148	Size of the file.
Aug 29 1997 17:49:36	Last modification date.
hampton/nitro/c7200-j-mz	Filename. Deleted files are indicated by square brackets around the filename.

Related Commands

Command	Description
cd	Changes the default directory or file system.
delete	Deletes a file on a Flash memory device.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

erase

To erase a file system, use the **erase** EXEC command. The **erase nvram:** command replaces the **write erase** command and the **erase startup-config** command.

erase *filesystem***:**

Syntax Description

filesystem:	File system name, followed by a colon. For example, **flash:** or **nvram:**

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

When a file system is erased, none of the files in the file system can be recovered.

The **erase** command can be used on both Class B and Class C Flash file systems only. To reclaim space on Flash file systems after deleting files using the **delete** command, you must use the **erase** command. This command erases all of the files in the Flash file system.

Class A Flash file systems cannot be erased. You can delete individual files using the **delete** EXEC command and then reclaim the space using the **squeeze** EXEC command. You can use the **format** EXEC command to format the Flash file system.

On Class C Flash file systems, space is dynamically reclaimed when you use the **delete** command. You can also use either the **format or erase** command to reinitialize a Class C Flash file system.

The **erase nvram:** command erases NVRAM. On Class A file system platforms, if the CONFIG_FILE variable specifies a file in Flash memory, the specified file will be marked "deleted."

Examples

The following example erases the NVRAM, including the startup configuration located there:

```
erase nvram:
```

The following example erases all of partition 2 in internal Flash memory:

```
Router# erase flash:2

System flash directory, partition 2:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
[1711152 bytes used, 15066064 available, 16777216 total]

Erase flash device, partition 2? [confirm]
Are you sure? [yes/no]: yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
```

The following example erases Flash memory when Flash is partitioned, but no partition is specified in the command:

```
Router# erase flash:

System flash partition information:
Partition    Size     Used     Free     Bank-Size     State        Copy-Mode
    1        4096K    2048K    2048K    2048K         Read Only    RXBOOT-FLH
    2        4096K    2048K    2048K    2048K         Read/Write   Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]
```

The system will prompt only if there are two or more read/write partitions. If the partition entered is not valid or is the read-only partition, the process terminates. You can enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?***number*) for directory display of a particular partition. The default is the first read/write partition.

```
System flash directory, partition 2:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]

Erase flash device, partition 2? [confirm] <Return>
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
delete	Deletes a file on a Flash memory device.
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

erase bootflash

The **erase bootflash:** and **erase bootflash** commands have identical functions. See the description of the **erase** command in this chapter for more information.

file prompt

To specify the level of prompting, use the **file prompt** global configuration command.

file prompt [**alert** | **noisy** | **quiet**]

Syntax Description

alert	(Optional) Prompts only for destructive file operations. This is the default.
noisy	(Optional) Confirms all file operation parameters.
quiet	(Optional) Seldom prompts for file operations.

Defaults

alert

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to change the amount of confirmation needed for different file operations.

This command affects only prompts for confirmation of operations. The router will always prompt for missing information.

Examples

The following example configures confirmation prompting for all file operations:

```
file prompt noisy
```

format

To format a Class A or Class C Flash file system, use the **format** EXEC command.

Class C Flash File System

format *filesystem1*:

Class A Flash File System

format [**spare** *spare-number*] *filesystem1*: [[*filesystem2*:][*monlib-filename*]]

Caution Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the Flash memory card can still be used. Otherwise, you must reformat the Flash card when some of the sectors fail.

Syntax Description

spare	(Optional) Reserves spare sectors as specified by the *spare-number* argument when formatting Flash memory.
spare-number	(Optional) Number of the spare sectors to reserve on formatted Flash memory. Valid values are from 0 to 16. The default value is zero.
filesystem1:	Flash memory to format, followed by a colon.
filesystem2:	(Optional) File system containing the monlib file to use for formatting filesystem1 followed by a colon.
monlib-filename	(Optional) Name of the ROM monitor library file (monlib file) to use for formatting the *filesystem1* argument. The default monlib file is the one bundled with the system software. When used with HSA and you do not specify the *monlib-filename* argument, the system takes ROM monitor library file from the slave image bundle. If you specify the *monlib-filename* argument, the system assumes that the files reside on the slave devices.

Defaults

The default monlib file is the one bundled with the system software.

The default number of spare sectors is zero (0).

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to format Class A or C Flash memory file systems.

In some cases, you might need to insert a new PCMCIA Flash memory card and load images or backup configuration files onto it. Before you can use a new Flash memory card, you must format it.

Sectors in Flash memory cards can fail. Reserve certain Flash memory sectors as "spares" by using the optional *spare* argument on the **format** command to specify 0 to 16 sectors as spares. If you reserve a small number of spare sectors for emergencies, you can still use most of the Flash memory card. If you specify 0 spare sectors and some sectors fail, you must reformat the Flash memory card, thereby erasing all existing data.

The monlib file is the ROM monitor library. The ROM monitor uses this file to access files in the Flash file system. The Cisco IOS system software contains a monlib file.

In the command syntax, *filesystem1:* specifies the device to format and *filesystem2:* specifies the optional device containing the monlib file used to format *filesystem1:*. If you omit the optional *filesystem2:* and *monlib-filename* arguments, the system formats *filesystem1:* using the monlib file already bundled with the system software. If you omit only *the optional filesystem2:* argument, the system formats *filesystem1:* using the monlib file from the device you specified with the **cd** command. If you omit only the optional *monlib-filename* argument, the system formats *filesystem1:* using the *filesystem2:* monlib file. When you specify both arguments—*filesystem2:* and *monlib-filename*—the system formats *filesystem1:* using the monlib file from the specified device. You can specify *filesystem1:*'s own monlib file in this argument. If the system cannot find a monlib file, it terminates its formatting.

⚠ **Caution** You can read from or write to Flash memory cards formatted for Cisco 7000 series Route Processor (RP) cards in your Cisco 7200 and 7500 series routers, but you cannot boot the Cisco 7200 and 7500 series routers from a Flash memory card formatted for the Cisco 7000 series routers. Similarly, you can read from or write to Flash memory cards formatted for the Cisco 7200 and 7500 series routers in your Cisco 7000 series routers, but you cannot boot the Cisco 7000 series routers from a Flash memory card formatted for the Cisco 7200 and 7500 series routers.

Examples

The following example formats a Flash memory card inserted in slot 0:

```
Router# format slot0:

Running config file on this device, proceed? [confirm]y
All sectors will be erased, proceed? [confirm]y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device slot0 completed
```

When the console returns to the EXEC prompt, the new Flash memory card is formatted and ready for use.

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
show file systems (Flash file system)	Lists available file systems.

Command	Description
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.
undelete	Recovers a file marked “deleted” on a Class A or Class B Flash file system.

fsck

To check a Class C Flash file system for damage and repair any problems, use the **fsck** EXEC command.

fsck [/nocrc] *filesystem*:

Syntax Description

/nocrc	(Optional) Omits cyclic redundancy checks (CRCs).
filesystem:	The file system to check.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is only valid on Class C Flash file systems.

Examples

The following example checks the Flash file system:

```
Router# fsck flash:

Fsck operation may take a while. Continue? [confirm]
flashfs[4]: 0 files, 2 directories
flashfs[4]: 0 orphaned files, 0 orphaned directories
flashfs[4]: Total bytes: 8128000
flashfs[4]: Bytes used: 1024
flashfs[4]: Bytes available: 8126976
flashfs[4]: flashfs fsck took 23 seconds.
Fsck of flash: complete
```

mkdir

To create a new directory in a Class C Flash file system, use the **mkdir** EXEC command.

mkdir *directory*

Syntax Description

directory	The name of the directory to create.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is only valid on Class C Flash file systems.

If you do not specify the directory name in the command line, the router prompts you for it.

Examples

The following example creates a directory named newdir:

```
Router# mkdir newdir

Mkdir file name [newdir]?
Created dir flash:newdir
Router# dir
Directory of flash:

  2  drwx          0   Mar 13 1993 13:16:21  newdir

8128000 bytes total (8126976 bytes free)
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
rmdir	Removes an existing directory in a Class C Flash file system.

more

To display a file, use the **more** EXEC command.

more [**/ascii** | **/binary** | **/ebcdic**] *file-url*

Syntax Description

/ascii	(Optional) Displays a binary file in ASCII format.
/binary	(Optional) Displays a file in hex/text format.
/ebcdic	(Optional) Displays a binary file in EBCDIC format.
file-url	The URL of the file to display.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

The **more system:running-config** command displays the same output as the **show running-config** command. The **more nvram:startup-config** command replaces the **show startup-config** command and the **show configuration** command.

You can use this command to display configuration files, as follows:

- The **more nvram:startup-config** command displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable. The Cisco IOS software informs you whether the displayed configuration is a complete configuration or a distilled version. A distilled configuration is one that does not contain access lists.
- The **more system:running-config** command displays the running configuration.

These commands show the version number of the software used when you last changed the configuration file.

You can display files on remote systems using the **more** command.

Examples

The following partial sample output displays the configuration file named startup-config in NVRAM:

```
Router# more nvram:startup-config

!
! No configuration change since last restart
! NVRAM config last updated at 02:03:26 PDT Thu Oct 2 1997
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service udp-small-servers
service tcp-small-servers
.
```

```
.
.
end
```

The following is partial sample output from the **more nvram:startup-config** command when the configuration file has been compressed:

```
Router# more nvram:startup-config

Using 21542 out of 65536 bytes, uncompressed size = 142085 bytes
!
version 12.1
service compress-config
!
hostname rose
!
.
.
.
```

The following partial sample output displays the running configuration:

```
Router2# more system:running-config

Building configuration...

Current configuration:
!
version 12.1
no service udp-small-servers
no service tcp-small-servers
!
hostname Router2
!
.
.
.
!
end
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
service compress-config	Compresses startup configuration files.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

pwd

To show the current setting of the **cd** command, use the **pwd** EXEC command.

pwd

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use the **pwd** command to show which directory or file system is specified as the default by the **cd** command. For all EXEC commands that have an optional *filesystem* argument, the system uses the file system specified by the **cd** command when you omit the optional *filesystem* argument.

For example, the **dir** command contains an optional *filesystem* argument and displays a list of files on a particular file system. When you omit this *filesystem* argument, the system shows a list of the files on the file system specified by the **cd** command.

Examples

The following example shows that the present working file system specified by the **cd** command is slot 0:

```
Router> pwd
slot0:/
```

The following example uses the **cd** command to change the present file system to slot 1 and then uses the **pwd** command to display that present working file system:

```
Router> cd slot1:
Router> pwd
slot1:/
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.

rename

To rename a file in a Class C Flash file system, use the **rename** EXEC command.

rename *url1 url2*

Syntax Description

url1	The original path and filename.
url2	The new path and filename.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is valid only on Class C Flash file systems.

Examples

In the following example, the file named Karen.1 is renamed test:

```
Router# dir

Directory of disk0:/Karen.dir/

  0  -rw-          0   Jan 21 1998 09:51:29  Karen.1
  0  -rw-          0   Jan 21 1998 09:51:29  Karen.2
  0  -rw-          0   Jan 21 1998 09:51:29  Karen.3
  0  -rw-          0   Jan 21 1998 09:51:31  Karen.4
243  -rw-        165   Jan 21 1998 09:53:17  Karen.cur

340492288 bytes total (328400896 bytes free)

Router# rename disk0:Karen.dir/Karen.1 disk0:Karen.dir/test
Router# dir

Directory of disk0:/Karen.dir/

  0  -rw-          0   Jan 21 1998 09:51:29  Karen.2
  0  -rw-          0   Jan 21 1998 09:51:29  Karen.3
  0  -rw-          0   Jan 21 1998 09:51:31  Karen.4
243  -rw-        165   Jan 21 1998 09:53:17  Karen.cur
  0  -rw-          0   Apr 24 1998 09:49:19  test

340492288 bytes total (328384512 bytes free)
```

rmdir

To remove an existing directory in a Class C Flash file system, use the **rmdir** EXEC command.

rmdir *directory*

Syntax Description

directory	Directory to delete.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is valid only on Class C Flash file systems.

Examples

The following example deletes the directory named newdir:

```
Router# dir

Directory of flash:

  2  drwx           0    Mar 13 1993 13:16:21   newdir

8128000 bytes total (8126976 bytes free)
Router# rmdir newdir
Rmdir file name [newdir]?
Delete flash:newdir? [confirm]
Removed dir flash:newdir
Router# dir
Directory of flash:

No files in directory

8128000 bytes total (8126976 bytes free)
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
mkdir	Creates a new directory in a Class C Flash file system.

show configuration

The **show configuration** command is replaced by the **show startup-config** and **more nvram:startup-config** commands. See the description of the **show startup-config** and **more** commands for more information.

show file descriptors

To display a list of open file descriptors, use the **show file descriptors** EXEC command.

show file descriptors

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

File descriptors are the internal representations of open files. You can use this command to learn if another user has a file open.

Examples

The following is sample output from the **show file descriptors** command:

```
Router# show file descriptors

File Descriptors:

   FD  Position  Open  PID  Path
    0    187392  0001    2  tftp://dirt/hampton/c4000-i-m.a
    1    184320  030A    2  flash:c4000-i-m.a
```

Table 27 describes the significant fields shown in the display.

Table 27 show file descriptors Field Descriptions

Field	Description
FD	File descriptor. The file descriptor is a small integer used to specify the file once it has been opened.
Position	Byte offset from the start of the file.
Open	Flags supplied when opening the file.
PID	Process ID of the process that opened the file.
Path	Location of the file.

show file information

To display information about a file, use the **show file information** EXEC command.

show file information *file-url*

Syntax Description

file-url	The URL of the file to display.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Examples

The following is sample output from the **show file information** command:

```
Router# show file information tftp://dirt/hampton/c2500-j-l.a

tftp://dirt/hampton/c2500-j-l.a:
  type is image (a.out) [relocatable, run from flash]
  file size is 8624596 bytes, run size is 9044940 bytes [8512316+112248+420344]
  Foreign image

Router# show file information slot0:c7200-js-mz

slot0:c7200-js-mz:
  type is image (elf) []
  file size is 4770316 bytes, run size is 4935324 bytes
  Runnable image, entry point 0x80008000, run from ram

Router1# show file information nvram:startup-config

nvram:startup-config:
  type is ascii text
```

Table 28 describes the possible file types.

Table 28 Possible File Types

Types	Description
image (a.out)	Runnable image in a.out format.
image (elf)	Runnable image in elf format.
ascii text	Configuration file or other text file.
coff	Runnable image in coff format.
ebcdic	Text generated on an IBM mainframe.
lzw compression	Lzw compressed file.
tar	Text archive file used by the Channel Interface Processor (CIP).

show file systems

To list available file systems, use the **show file systems** command in EXEC mode.

show file systems

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

Use this command to learn the alias names (Prefixes) of the file systems your router supports.

Examples

The following is sample output from the **show file systems** command:

```
Router# show file systems

File Systems:

     Size(b)       Free(b)   Type     Flags  Prefixes
          -             -   opaque    rw     null:
          -             -   opaque    rw     system:
          -             -   opaque    ro     xmodem:
          -             -   opaque    ro     ymodem:
          -             -  network    rw     tftp:
          -             -  network    rw     rcp:
          -             -  network    rw     ftp:
*    4194304       4190616    flash    rw     flash:
      131066        129185    nvram    rw     nvram:
          -             -   opaque    wo     lex:
```

Table 29 describes the significant fields shown in the display.

Table 29 show file systems Field Descriptions

Type	Description
Size(b)	Amount of memory in the file system (in bytes).
Free(b)	Amount of free memory in the file system (in bytes).
Type	Type of file system.
Flags	Permissions for file system.
Prefixes	Alias for file system.
disk	The file system is for a rotating medium.
flash	The file system is for a Flash memory device.

Table 29 show file systems Field Descriptions (continued)

Type	Description
network	The file system is a network file system (TFTP, rcp, FTP, and so on).
nvram	The file system is for an NVRAM device.
opaque	The file system is a locally generated “pseudo” file system (for example, the “system”) or a download interface, such as brimux.
rom	The file system is for a ROM or EPROM device.
tty	The file system is for a collection of terminal devices.
unknown	The file system is of unknown type.

Table 30 describes file system flags.

Table 30 Possible File System Flags

Flag	Description
ro	The file system is Read Only.
rw	The file system is Write Only.
wo	The file system is Read/Write.

squeeze

To permanently erase files tagged as “deleted” or “error” on Class A Flash file systems, use the **squeeze** command in EXEC mode.

squeeze [/nolog] [/quiet] *filesystem*:

Syntax Description

/nolog	(Optional) Disables the squeeze log (recovery data) and accelerates the squeeze process.
/quiet	(Optional) Disables status messages during the squeeze process.
filesystem:	The Flash file system, followed by a colon. Typically **flash:** or **slot0:**.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(1)	This command was implemented in images for the Cisco 2600 and Cisco 3600 series.
12.2(4)XL	This command was implemented in images for the Cisco 1700 series.
12.1(9), 12.0(17)S 12.0(17)ST, 12.2(2), 12.2(2)T, 12.2(2)B, 12.1(9)E	The **/nolog** and **/quiet** keywords were added.

Usage Guidelines

When Flash memory is full, you might need to rearrange the files so that the space used by the files marked “deleted” can be reclaimed. (This “squeeze” process is required for linear Flash memory cards to make sectors contiguous; the free memory must be in a “block” to be usable.)

When you enter the **squeeze** command, the router copies all valid files to the beginning of Flash memory and erases all files marked “deleted.” After the squeeze process is completed, you can write to the reclaimed Flash memory space.

⚠ **Caution** After performing the squeeze process you cannot recover deleted files using the **undelete** EXEC mode command.

In addition to removing deleted files, the **squeeze** command removes any files that the system has marked as “error”. An error file is created when a file write fails (for example, the device is full). To remove error files, you must use the **squeeze** command.

Rewriting Flash memory space during the squeeze operation may take several minutes.

Using the **/nolog** keyword disables the log for the squeeze process. In most cases this will speed up the squeeze process. However, if power is lost or the Flash card is removed during the squeeze process, all the data on the Flash card will be lost, and the device will have to be reformatted.

7827
a

Note Using the **/nolog** keyword makes the squeeze process uninterruptible.

Using the **/quiet** keyword disables the output of status messages to the console during the squeeze process.

If the optional keywords are not used, the progress of squeeze process will be displayed to the console, a log for the process will be maintained, and the squeeze process is interruptible.

On Cisco 2600 or Cisco 3600 series routers, the entire file system needs to be erased once before the **squeeze** command can be used. After being erased once, the **squeeze** command should operate properly on the Flash file system for the rest of the Flash file system's history.

To erase an entire flash file system on a Cisco 2600 or 3600 series router, perform the following steps:

Step 1 If the Flash file system has multiple partitions, enter the **no partition** command to remove the partitions. The reason for removing partitions is to ensure that the entire Flash file system is erased. The **squeeze** command can be used in a Flash file system with partitions after the Flash file system is erased once.

Step 2 Enter the **erase** command to erase the Flash file system.

Examples

In the following example, the file named "config1" is deleted, and then the **squeeze** command is used to reclaim the space used by that file. The **/nolog** option is used to speed up the squeeze process.

```
Router# delete config1
Delete filename [config1]?
Delete slot0:conf? [confirm]
Router# dir slot0:
! Note that the deleted file name appears in square brackets
Directory of slot0:/

    1  -rw-     4300244   Apr 02 2001 03:18:07  c7200-boot-mz.122-0.14
    2  -rw-        2199   Apr 02 2001 04:45:15  [config1]
    3  -rw-     4300244   Apr 02 2001 04:45:23  image
20578304 bytes total (11975232 bytes free)
!20,578,304 - 4,300,244 - 4,300,244 - 2,199 - 385 = 11975232


Router# squeeze /nolog slot0:
%Warning: Using /nolog option would render squeeze operation uninterruptible.
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]

Squeeze of slot0 completed in 291.832 secs .
Router# dir slot0:
Directory of slot0:/

    1  -rw-     4300244   Apr 02 2001 03:18:07  c7200-boot-mz.122-0.14
    2  -rw-     4300244   Apr 02 2001 04:45:23  image

20578304 bytes total (11977560 bytes free)
!20,578,304 - 4,300,244 - 4,300,244 - 256 = 11977560
```

Related Commands

Command	Description
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

undelete

To recover a file marked “deleted” on a Class A or Class B Flash file system, use the **undelete** EXEC command.

undelete *index* [*filesystem*:]

Syntax Description

index	A number that indexes the file in the **dir** command output.
filesystem:	(Optional) A file system containing the file to undelete, followed by a colon.

Defaults

The default file system is the one specified by the **cd** command.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

For Class A and B Flash file systems, when you delete a file, the Cisco IOS software simply marks the file as deleted, but it does not erase the file. This command allows you to recover a “deleted” file on a specified Flash memory device. You must undelete a file by its index because you could have multiple deleted files with the same name. For example, the “deleted” list could contain multiple configuration files with the name router-config. You undelete by index to indicate which of the many router-config files from the list to undelete. Use the **dir** command to learn the index number of the file you want to undelete.

You cannot undelete a file if a valid (undeleted) file with the same name exists. Instead, you first delete the existing file and then undelete the file you want. For example, if you had an undeleted version of the router-config file and you wanted to use a previous, deleted version instead, you could not simply undelete the previous version by index. You would first delete the existing router-config file and then undelete the previous router-config file by index. You can delete and undelete a file up to 15 times.

On Class A Flash file systems, if you try to recover the configuration file pointed to by the CONFIG_FILE environment variable, the system prompts you to confirm recovery of the file. This prompt reminds you that the CONFIG_FILE environment variable points to an undeleted file. To permanently delete all files marked “deleted” on a Flash memory device, use the **squeeze** EXEC command.

On Class B Flash file systems, you must use the **erase** EXEC command to recover any space taken up by deleted files.

Examples

The following example recovers the deleted file whose index number is 1 to the Flash memory card inserted in slot 0:

```
undelete 1 slot0:
```

Related Commands

Command	Description
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.

verify

To verify the checksum of a file on a Flash memory file system, use the **verify** EXEC command.

verify *filesystem*:[*file-url*]

Syntax Description

filesystem:	Flash memory file system containing the files to list, followed by a colon. Standard file system keywords for this command include **flash:**, **bootflash:**, and **slot0:**.
file-url	(Optional) URL of the file to verify. Generally this consists only of the filename(s), but you may also specify directories (file paths), separated by forward-slashes (/). The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Defaults

The current working device is the default device.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command replaces the **copy verify** and **copy verify flash** commands.

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into Flash memory; it is not displayed when the image file is copied from one disk to another.

To display the contents of Flash memory, use the **show flash** command. The Flash contents listing do not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into Flash memory, use the **verify** command.

Note The verify command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the router and saved in the file system without detection.
To verify that a Cisco IOS software image was not corrupted while it was transfered to the router, copy the image from where it is stored on your router to a Unix server. Also copy the same image from CCO (Cisco.com) to the same Unix server. (The name may need to be modified if you try to save the image in the same directory as the image that you copied from the router.) Then run a Unix **diff** command on the two Cisco IOS software images. If there is no difference then the image stored on the router has not been corrupted.

Examples

The following example verifies that the file named c7200-js-mz is on the Flash memory card inserted in slot 0:

```
Router# dir slot0:
Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  5  -rw-         639   Oct 02 1997 12:09:32  rally
  7  -rw-         639   Oct 02 1997 12:37:13  the_time

20578304 bytes total (3104544 bytes free)
tw3-7200-1# verify slot0:
Verify filename []? c7200-js-mz
Verified slot0:
```

The following example also verifies that the file named c7200-js-mz is on the Flash memory card inserted in slot 0:

```
Router# verify slot0:?
slot0:c7200-js-mz  slot0:rally slot0:hampton/nitro/c7200-j-mz  slot0:the_time

Router# verify slot0:c7200-js-mz
Verified slot0:c7200-js-mz
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination, use the copy EXEC command.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the **cd** command.
show file systems	Lists available file systems.

write erase

The **write erase** command is replaced by the **erase nvram:** command. See the description of the **erase** command in this chapter for more information.

write terminal

The **more system:running-config** command replaces the **write terminal** command. See the description of the **more** command in this chapter for more information.

AP 65

Smart Serial Connector Cables

The following cables are specific to the new dual-serial port WAN interface cards and feature Cisco's new, compact, high-density Smart Serial connector to support a wide variety of electrical interfaces when used with the appropriate transition cable. Two cables are required to support the two ports on the WIC. Each port on a WIC can support a different physical interface (protocol and DTE/DCE).

Table 9-9: Smart Serial Connector Cables

WAN Interface Card	Cable Type	Product Number	Length	Gender
WIC-2A/S (up to 128 kbps Sync or 115.2 kbps Async)	V.35 DTE	CAB-SS-V35MT(=)	10 ft (3.048 m)	Male
WIC-2T (high speed serial)	V.35 DCE	CAB-SS-V35FC(=)	10 ft (3.048 m)	Female
	RS-232 DTE	CAB-SS-232MT(=)	10 ft (3.048 m)	Male
	RS-232 DCE	CAB-SS-232FC(=)	10 ft (3.048 m)	Female
	RS-449 DTE	CAB-SS-449MT(=)	10 ft (3.048 m)	Male
	RS-449 DCE	CAB SS-449FC(=)	10 ft (3.048 m)	Female
	X.21 DTE	CAB-SS-X21MT(=)	10 ft (3.048 m)	Male
	X.21 DCE	CAB-SS-X21FC(=)	10 ft (3.048 m)	Female
	RS-530 DTE	CAB-SS-530MT(=)	10 ft (3.048 m)	Male
	RS-530 A DTE	CAB-SS-530AMT(=)	10 ft (3.048 m)	Male

AP GF

CHAPTER 1

Overview of Cisco 3700 Series Routers

Cisco 3700 series routers are modular access routers with LAN and WAN connections that can be configured by means of interchangeable network modules and interface cards.

This chapter describes the features and specifications of the routers and includes the following sections:

Hardware Features

Cisco 3700 series includes the Cisco 3725 and the Cisco 3745 routers, which provide the following features:

- Cisco 3700 compact Flash cards
- Advanced integration module (AIM) slots
- Support for double-width network modules
- Two sockets for synchronized DRAM (SDRAM)
- User-configurable memory (shared memory or processor memory)
- Two FastEthernet ports
- High-speed console and auxiliary ports (up to 115.2 kbps)

Cisco 3725

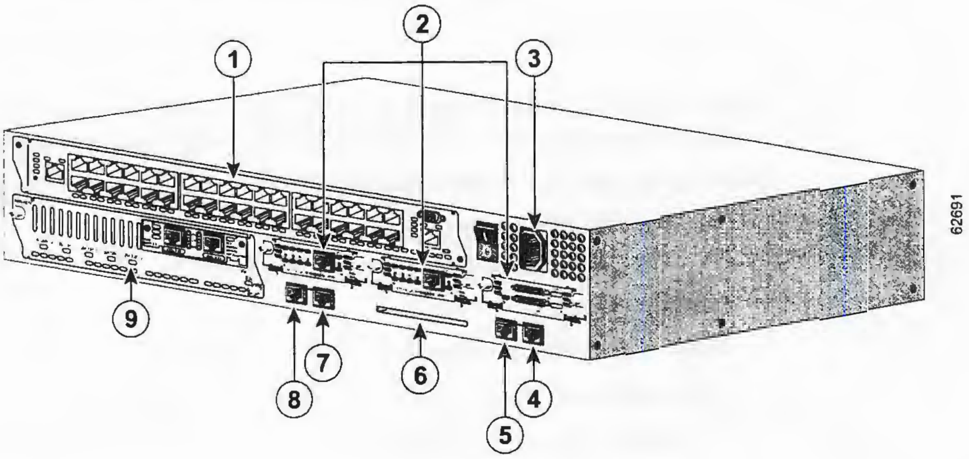
Cisco 3725 routers include the following additional features:

- High-performance 240-MHz Reduced Instruction Set Computer (RISC) processor
- Up to 256 MB SDRAM
- Up to 128 MB Flash memory
- Two slots for network modules, one of which can accommodate a double-width network module
- Three interface card slots

- Two Cisco 3700 compact Flash slots (one external and one internal)
- Two AIM slots
- Can be installed in a 19- or 23-inch rack or on a desk
- Supports the Cisco Redundant Power System
- 2 rack units (RU) chassis height

Figure 1-1 shows the rear panel of the Cisco 3725.

Figure 1-1 Rear Panel of the Cisco 3725 Router



1	Double-width network module slot	6	Compact Flash slot
2	Interface card slots	7	FastEthernet 0/0 port
3	Power supply	8	FastEthernet 0/1 port
4	Auxiliary port	9	Single-width network module slot
5	Console port		

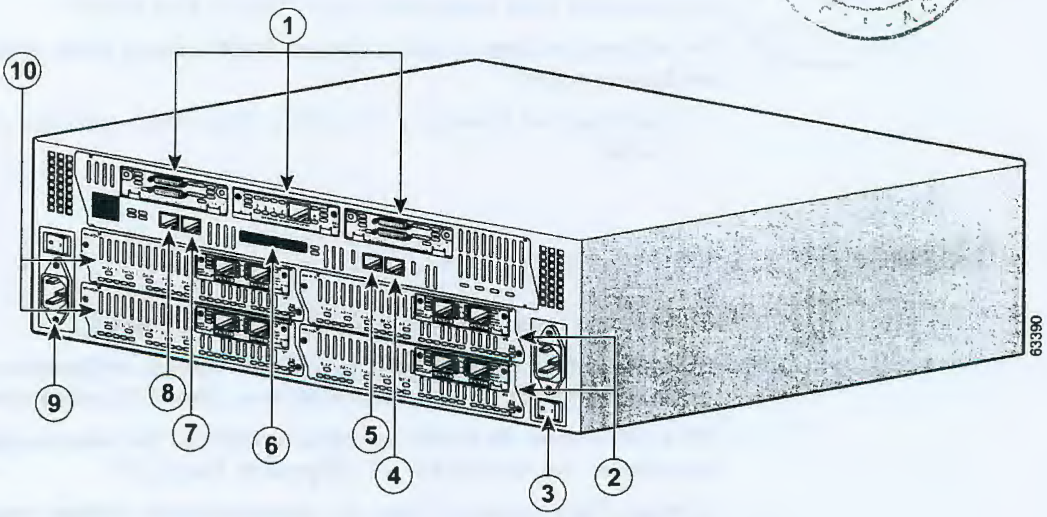
Cisco 3745

Cisco 3745 routers include the following additional features:

- High-performance 350-MHz RISC processor
- Up to 256 MB SDRAM
- Up to 128 MB Flash memory
- Four slots for network modules that can accommodate up to two double-width network modules
- Three interface card slots
- Two Cisco 3700 compact Flash slots (one external and one internal)
- Two AIM slots
- Can be installed in a 19- or 23-inch rack or on a desk
- Supports the Cisco Redundant Power System
- 3 rack units (RU) chassis height

Figure 1-2 shows the rear panel of the Cisco 3745.

Figure 1-2 Rear Panel of the Cisco 3745 Router



1	Interface card slots	**6**	Cisco 3700 compact Flash slot
2	Network modules	**7**	Auxiliary port
3	Power supply	**8**	Console port
4	FastEthernet 0/0 port	**9**	Power supply
5	FastEthernet 0/1 port	**10**	Network modules

Modules, Interface Cards, and Memory

The latest information on network modules, WAN interface cards (WICs), voice interface cards (VICs), advanced integration modules (AIMs), and memory is available online and on the documentation CD-ROM.

- For information on installing network modules, refer to the following documents:
  - *Quick Start Guide: Network Modules for Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*
  - *Cisco Network Modules Hardware Installation Guide*
- For information on installing WICs and VICs, refer to the following documents:
  - *Quick Start Guide: Interface Cards for Cisco 1600, 1700, 2600, 3600, and 3700 Series*
  - *Cisco Interface Cards Hardware Installation Guide*
- For information on installing AIMs, refer to the following documents:
  - *AIM Installation Quick Start Guide: Cisco 2600, 3600, and 3700 Series*
  - *Installing Advanced Integration Modules in Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers*

- For information about installing DRAM, SDRAM, NVRAM, and Flash memory SIMMs, refer to the following hardware configuration notes:
  - *Upgrading System Memory in Cisco 3700 Series Routers*
  - *Installing Field Replaceable Units in Cisco 3745 Routers*
- For information about installing compact Flash memory cards, refer to the following hardware configuration note:
  - *Installing and Formatting Cisco 2691, Cisco 3631, and Cisco 3700 Compact Flash Memory Cards*

Memory

Cisco 3700 series routers support the following types of memory:

- SDRAM—Serves two functions: It stores the running configuration and routing tables and is used for packet buffering by the network interfaces. Cisco IOS software executes from SDRAM memory.
- NVRAM—Stores the system configuration file and the virtual configuration register. (For more information, see Appendix C, "Configuration Register.")
- Compact Flash memory—Stores the operating system software image. You can increase compact Flash memory by adding Cisco 3700 compact Flash cards. Refer to the *Installing and Formatting Cisco 3631, and Cisco 3700 Compact Flash Memory Cards* document.
- EPROM-based memory—Stores the ROM monitor, which allows you to boot an operating system software image from Flash memory or Cisco Flash.

Table 1-1 and Table 1-2 list processor and memory specifications for Cisco 3700 series routers.

Table 1-1 Cisco 3725 Router Processor and Memory Specifications

Description	Specification
Processor	240-MHz PMC-Sierra RM7061A RISC processor
SDRAM	128 to 256 MB
NVRAM	56 KB
Compact Flash	32, 64, or 128 MB
Boot ROM	512 KB

Table 1-2 Cisco 3745 Router Processor and Memory Specifications

Description	Specification
Processor	350-MHz PMC-Sierra RM7000A RISC processor
SDRAM	128 to 256 MB
NVRAM	152 KB
Compact Flash	32, 64, or 128 MB
Boot ROM	704 KB

Power Supply Options

Table 1-3 lists the power supply options supported by Cisco 3700 series routers. Depending on the configuration specified when you placed your order, your router may not support all of these options.

Table 1-3 Power Supply Options for Cisco 3700 Series Routers

Power Supply Option	Cisco 3725	Cisco 3745
AC input power	Yes	Yes
DC input power	No	Yes
–48V telephony power module provides inline power to IP phones	Yes	Yes
Dual hot-swappable power supplies	No	Yes[1]
Compatible with Cisco Redundant Power System	Yes	Yes

[1] Due to increased power consumption in high-temperature environments, a fully loaded Cisco 3745 requires both power supplies when ambient temperature exceeds 40°C. Cisco 3745 routers operating under these conditions do not support the online replacement of power supplies.

Internal –48V Telephony Power Modules

Cisco 3700 series routers provide inline power to IP phones connected to the router through Ethernet Switch Network Modules. This power is supplied by special –48V modules that connect directly to the chassis power supplies in Cisco 3725 and Cisco 3745 routers. A single –48V power module meets the power needs of up to 36 IP phones. A Cisco 3745 router with two –48V power modules installed provides redundant power for up to 36 IP phones. Figure 1-3 and Figure 1-4 show the –48V power modules as they appear when installed in Cisco 3700 series routers.

Figure 1-3 Cisco 3725 Router with Optional –48V Power Module Installed

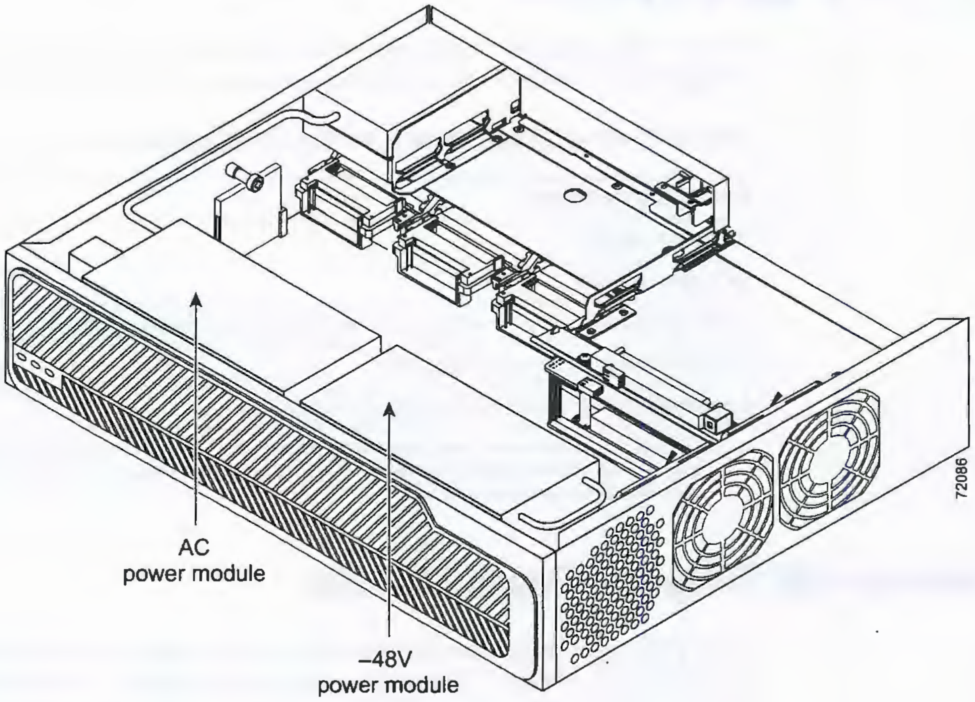
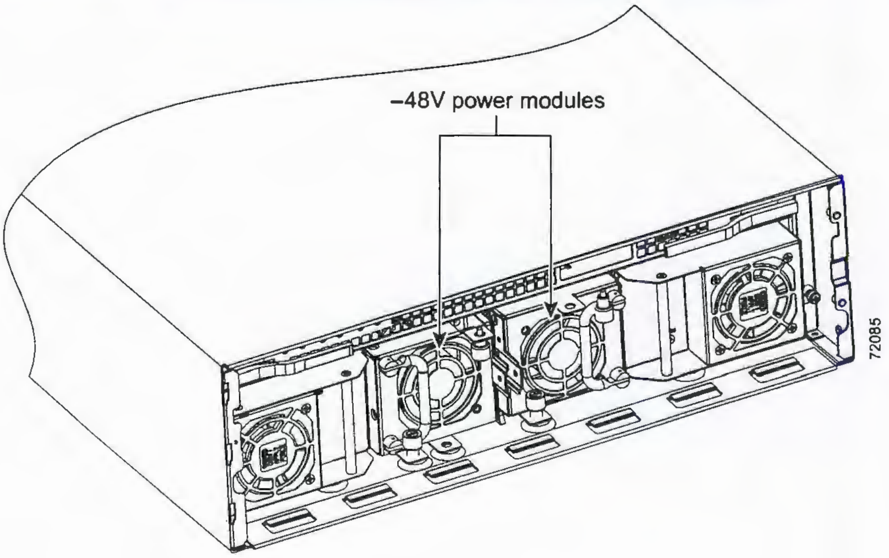


Figure 1-4 Cisco 3745 Router with Optional –48V Power Modules Installed



System Specifications

Table 1-4 and Table 1-5 list Cisco 3700 series system specifications.

Table 1-4 Cisco 3725 Router System Specifications

Description	Specification
Dimensions (H x W x D)	3.5 x 17.1 x 15.0 in. (8.9 x 43.4 x 38.1 cm), 2 RU chassis height
Weight	14 lb (6.4 kg)
Input voltage, AC power supply Frequency Input surge current (AC)	100 to 240 VAC, autoranging 47 to 63 Hz 50 A maximum, one cycle (–48 V power module included)
Power dissipation	135 W (maximum)
Console and auxiliary ports	RJ-45 connector
Operating humidity	5 to 95%, noncondensing
Operating temperature	32 to 104°F (0 to 40°C)
Nonoperating temperature	–40 to 162°F (–40 to 72°C)
Noise level	52 dBA (maximum)
Regulatory compliance	FCC Part 15 Class A. For additional compliance information, refer to the *Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Regulatory Compliance and Safety Information* document that accompanied the router.
Safety compliance	UL 60950; CAN/CSA C22.2 No. 60950-00; IEC 60950, EN 60950; AS/NZS 3260; TS001

Table 1-5 Cisco 3745 Router System Specifications

Description	Specification
Dimensions (H x W x D)	5.25 x 17.25 x 15.00 in. (13.3 x 43.8 x 38.1 cm), 3 RU chassis height
Weight	32 lb (14.5 kg), including chassis and four network modules
Input voltage, AC power supply Frequency Input surge current (AC)	100 to 240 VAC, autoranging 47 to 63 Hz 80 A maximum, one cycle (–48 V power module included)
Input rating, DC power supply Operational between Input surge current (DC)	–48 to –60 VDC, 10 A maximum –38 to –75 VDC, 10 A maximum 50 A, <10 ms
Power dissipation	230 W (maximum)
Console and auxiliary ports	RJ-45 connector
Operating humidity	5 to 95%, noncondensing
Operating temperature	32 to 104°F (0 to 40°C)[1]
Nonoperating temperature	–40 to 162°F (–40 to 72°C)
Noise level	60 dBA (maximum)
Regulatory compliance	FCC Part 15 Class A. For additional compliance information, refer to the *Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Regulatory Compliance and Safety Information* document that accompanied the router.
Safety compliance	UL 60950; CAN/CSA C22.2 No. 60950-00; IEC 60950, EN 60950; AS/NZS 3260; TS001

[1] Due to increased power consumption in high-temperature environments, a fully loaded Cisco 3745 requires both power supplies when ambient temperature exceeds 40°C.

Regulatory Compliance

For compliance information, refer to the *Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Regulatory Compliance and Safety Information* document that accompanied the router.

AP 66

CISCO SYSTEMS

Cisco Products
Quick Reference Guide

April 2003

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-785983
Text Part Number: 78-5983-11

Cisco Products Quick Reference Guide

General Disclaimer

Although Cisco has attempted to provide accurate information in this Guide, Cisco assumes no responsibility for the accuracy of the information. Cisco may change the programs or products mentioned at any time without prior notice. Mention of non-Cisco products or services is for information purposes only and constitutes neither an endorsement nor a recommendation of such products or services or of any company that develops or sells such products or services.

ALL INFORMATION PROVIDED ON THIS WEB SITE IS PROVIDED "AS IS," WITH ALL FAULTS, AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

CISCO AND ITS SUPPLIERS SHALL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR REVENUES, COSTS OF REPLACEMENT GOODS OR SERVICES, LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OF THE GUIDE OR ANY CISCO PRODUCT OR SERVICE, OR DAMAGES RESULTING FROM USE OF OR RELIANCE ON THE INFORMATION PROVIDED, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Many of the Cisco products and services identified in this Guide are provided with written software licenses and limited warranties. Those licenses and warranties provide the purchasers of those products with certain rights. Nothing in this Guide shall be deemed to expand, alter, or modify any warranty or license provided by Cisco with any Cisco product, or to create any new or additional warranties or licenses.

CONTENTS

Introduction

CHAPTER 2 LAN Switching

CHAPTER 3 Wireless LAN Products

CHAPTER 4 IP Telephony, Video, & Web Collaboration

CHAPTER 7 Broadband and Dial Access Products

Introduction

Cisco Products Quick Reference Guide (CPQRG)

CPQRG Background

The Cisco Products Quick Reference Guide (CPQRG) is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many of Cisco's products. The CPQRG is primarily published to support Cisco partners, resellers, sales account teams, and even end-user customers who need a broad, high-level overview of Cisco products, but at that moment do not have access to Cisco's Web site, the Cisco Connection Online (CCO) at **http://www.cisco.com**.

Because this book is only published twice per year, there are likely to be new products, configurations, and part numbers not included in this edition. Note: For the most up-to-date and comprehensive information about Cisco products and solutions, please refer to our on-line information or consult a Cisco representative.

CPQRG Ordering Information

Additional printed copies of this book can be purchased on an as-needed basis or through an annual subscription. To order, see **http://shop.cisco.com/login**.

For questions regarding the CPQRG ordering process, please send an email to **companystore@external.cisco.com**.

For questions, comments or to download an Adobe PDF version of the CPQRG, go to **http://www.cisco.com/go/guide**.

How to Get More Complete Product Information

Cisco Product Catalog	For more comprehensive information on all of Cisco's products, please refer to the Cisco Product Catalog at: http://www.cisco.com/univercd/cc/td/doc/pcat/
Cisco Connection Online (CCO)	For even more complete product and solution information, please go to CCO at http://www.cisco.com. In addition to product, technology, and network solutions support, CCO provides a wealth of information including how to find an authorized repesentative or partner, how to order products, technical support/customerservice, Cisco Corporate news and information, and links to training/events/seminars.

Cisco Systems Overview

Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Cisco's Internet Protocol-based (IP) networking solutions are the foundation of the Internet and most corporate, education, and government networks around the world. Cisco provides the broadest line of solutions for transporting data, voice and video within buildings, across campuses, or around the world.

Today, the Internet and computer networking are an essential part of business, learning and personal communications and entertainment. Virtually all messages or transactions passing over the Internet are carried quickly and securely through Cisco equipment. Cisco solutions ensure that networks both public and private operate with maximum performance, security, and flexibility. In addition, Cisco solutions are the basis for most large, complex networks used by corporations, public institutions, telecommunication companies, and are found in a growing number of medium-sized commercial enterprises.

Cisco was founded in 1984 by a group of computer scientists from Stanford University. Since the company's inception, Cisco engineers have been prominent in advancing the development of IP- the basic language to communicate over the Internet and in private networks. The company's tradition of innovation continues today with Cisco creating leading products and key technologies that will make the Internet more useful and dynamic in the years ahead. These technologies include: advanced routing and switching, voice and video over IP, optical networking, wireless, storage networking, security, broadband, and content networking.

In addition to technology and product leadership, Cisco is recognized as an innovator in how business is conducted. The company has been a pioneer in using the Internet to provide customer support, sell products, offer training, and manage finances. Drawing upon the company's own Internet best practices and core-value of customer focus, Cisco has established the Internet Business Solutions Group (IBSG) dedicated to helping top business leaders transform their own businesses into e-businesses.

As a company, Cisco operates on core values of customer focus and corporate citizenship. The company's philanthropic efforts are committed to helping communities prosper while also encouraging Cisco employees to learn about the needs of the communities where Cisco operates. Also, to help bolster education around the world, the company has founded Cisco Networking Academies in 128 countries dedicated to teaching students to design, build, and maintain computer networks.

Cisco Channel Partner Program

Whether you provide services, solutions or a combination of both, Cisco is committed to your success. The Cisco Channel Partner Program can help partners create a sustainable business model in a fast-changing environment, where customers require value-added services, focused technical expertise, and higher levels of satisfaction. As a Cisco certified partner, you'll have the backing of the Cisco brand, and access to world-class products and service packages, technical support, productivity tools, online training, marketing resources and sales promotions.

The Partner Program integrates the technology focus of each Cisco Partner Specialization, flexible individual career certification requirements, customer satisfaction targets, and pre- and post-sales support capabilities. These elements make up the points-based structure of the overall program requirements. There are three partner certification levels: Gold Certification, Silver Certification, and Premier Certification.

The Partner Program requires every partner to specialize in technology areas as part of the program requirement. You may choose the technology area for Specialization, but must earn a minimum number of Specialization points to become certified. You may decide to be strictly a specialized partner or specialize your organization as a means to achieving certification. Either way, you'll have access to structured training roadmaps, free online technical and sales education and video-on-demand content to build your knowledge and skill level through the Partner E-Learning Connection **http://cisco.partnerelearning.com**

For More Information

See the Channel Partner Program Web Site:
http://www.cisco.com/go/channelprograms
If you are interested in reselling Cisco product without becoming certified or specialized, see **http://www.cisco.com/go/reseller**

Reseller and Customer Support

Reseller Sales and Technical Assistance Contact Information

Customer Help Lines	Contact Information
US Distribution Presales Helplines[1]	Comstor: 800-COMSTOR, option 3 Ingram Micro: 800-445-5066, enter Ingram customer #, dial extension 24041 Tech Data: 800-237-8931, extension 77776
Presales—Partner/Reseller Helpline	800 553-6387 (within U.S.) 408 526-7208 (outside U.S.) http://CiscoPartner.custhelp.com/
Post-Sales—Technical Assistance Center (TAC)	800 553-6387 (within U.S.) 408 526-7209 (outside U.S.) tac@cisco.com (e-mail)

[1] Follow voice prompts to access: Pre-sales Assistance of Network Validation & Product Information, Reseller Support, Customer Service, Service Contract Sales, Reporting a technical problem/open a trouble ticket, and Seminars, Events, Training & Certification

Helpful Cisco Web Sites

Cisco Web Site	URL[1]
Worldwide Contacts Cisco office bcations; directions; maps; and sales, partners, and channel contacts.	http://www.cisco.com/go/wwcontacts
Partner Relationship Central Find a Channel Account Manager (CAM), Distributor, apply to the Cisco Channel Partner Program, or update your profile.	http://www.cisco.com/go/prc
Technical Support For customer support tips, software center, online documents, and more.	http://www.cisco.com/go/support http://www.cisco.com/public/Tech_support.shtml http://www.cisco.com/public/technotes/serv_tips.shtml
Cisco Products Quick Reference Guide This guide is available on line (in PDF and HTML); it is continually updated between bi-yearly printings. CCO login required.	http://www.cisco.com/go/guide
Cisco Subscription Service Ordering service for one-time purchase of or annual subscriptions to this guide or other Cisco documents and CDs; order online, or order by phone by calling 800 768-7162 (U.S. or Canada) or 925 327-4072 (outside the U.S.).	http://shop.ciscocom/login
Partner Help Search partners' frequently asked questions and ask for the help you need	http://ciscopartnercusthelp.com/
Certification/Specialization Application Apply for a Cisco Certification or Specialization	http://www.cisco.com/warp/customer/765/partner_programs/apply/
Find a Channel Account Manager Search for the CiscoChannel Account Manager assigned to your company	http://tools.cisco.com/WWChannels/CAMLOC/jsp/cam_locator.jsp
Partner Registration Begin your relationship with Cisco by registering as a Cisco Registered or Certified Partner	http://tools.cisco.com/WWChannels/GETLOG/jsp/GetLoginjsp?page=PartnerUserHomePage
Tool Index	http://www.cisco.com/en/US/partners/partners_tool_index.html
Get CCO Access Register for a guest-level Cisco.com ID as a prerequisite for partner level access	http://tools.cisco.com/RPF/register/register.do
Associate Myself With A Partner If you are an employee of Cisco Registered and Cisco Certified or Specialized Partners, you can associate yourself with your company and upgrade your current Cisco.com ID to partner level	http://tools.cisco.com/WWChannels/GETLOG/jsp/GetLoginjsp?page=PartnerUserHomePage
Partner Self Service Use this suite of tools to manage personal and company information in the Cisco partner database	http://tools.cisco.com/WWChannels/GETLOG/welcome.do
Update Company Data If you are a registered partner administrator, you can update company and contact information	http://www.cisco.com/warp/public/765/tools/certification/
Worldwide Distributors Web Site List, by country, of authorized Cisco Distributors who stock and resell Cisco products.	http://www.cisco.com/go/disti
Distribution Product Reference Guide (DPRG) Complete list of pricing information, part numbers, and more for distribution (2-tier) products. Data is refreshed nightly. CCO login required.	http://www.cisco.com/dprg
Partner Business Central—Browse and Configure Products An ecommerce web site with a configuration tool to validate channel product options, also select and compare products, check price and availability, and submit your order to your distributor online. CCO login required—click on "Browse and Configure Products".	http://www.cisco.com/go/partner/bizcentral
End-of-Life Matrix Last order and end-of-life dates for Cisco products	http://www.cisco.com/go/eol
Training Cisco University—Offers detailed course material on the latest technical topics throughout the year targeted for Resellers, Partners and Cisco Sales representatives. Also see the Partner E-learning Connection.	http://www.cisco.com/go/ciscou http://cisco.partnerelearning.com

[1] Additional CCO access required for most URLs.

Partner and Reseller Service and Support Offerings

Various partner and reseller service and support programs are available according to certification level and method of purchase from Cisco:

Method of Purchase	Service and Support Offerings
Direct from Cisco (only available to Partners with Direct contracts)	• *System Integrator Support*—System Integrator Support 98 (SIS98) program is designed for Silver and Gold partners who wish to provide their own brand of support to their end customers with back-end support from Cisco – SMARTspares provides partners using SIS98 the opportunity to leverage Cisco's logistics infrastructure to provide their customers with enhanced delivery services. • *Shared Support*—Currently only available in the US, Cisco's Shared Support program is designed for Silver and Gold partners who wish to provide their own brand of support to their end customers while leveraging Cisco's Technical Assistance Center (TAC) and logistics infrastructure • *Cisco Brand Resale*—Program allows partners to provide Cisco's services (SMARTnet, etc.) directly to their end customers
2-Tier (through a Distributor)	• *Packaged Services*—Partners and Resellers may purchase warranty extension, hardware replacement, installation and configuration, technical support, software upgrades, and online services. Several of these services have been bundled together to offer convenient service solutions for Cisco customers.

Packaged Resalable Service Products (only via Distributors/2-Tier):

Product	Description
Maintenance Services	
SMARTnet Maintenance	Provides customers with software maintenance, registered access to CCO, advance replacement of hardware, and technical support required for self-maintenance. SMARTnet maintenance has three delivery options: • SMARTnet 8x5xNBD (Next Business Day)—8 hours/day, 5 days/week, next-business-day hardware replacement • SMARTnet 8x5x4—8 hours/day, 5 days/week, 4-hour hardware replacement • SMARTnet 24x7x4—24 hours/day, 7 days/week, 4-hour hardware replacement Available through resellers and distributors.
SMARTnet Onsite	Provides all the benefits of SMARTnet maintenance, plus one of the following onsite hardware services for repairs: • SMARTnet Onsite 8x5xNBD—8 hours/day, 5 days/week, next-business-day response • SMARTnet Onsite 8x5x4—8 hours/day, 5 days/week, 4-hour response • SMARTnet Onsite 24x7x4—24 hours/day, 7 days/week, 4-hour response Packaged SMARTnet OnSite 24x7x4 provides SMARTnet OnSite 24x7x4 service in a shrink-wrapped package, allowing it to be effectively marketed through resellers.
Cisco Advance Replacement	Advance Replacement offers customers the flexibility to cover their equipment with an advance replacement service only. Cisco Advance Replacement comes with a full year of advance replacement coverage, guest access to the public portion of Cisco Connection Online (CCO), and a single technical support incident. This service is intended to be used by customers who need to supplement service offered by their reseller with a replacement option from Cisco.
Software Application Support plus Upgrades (SASU)	Software Application Support plus Upgrades provides customers with software upgrades and maintenance releases for Cisco Application Software, registered access to Cisco.com plus technical support, for one year. For when a customer needs investment protection on software purchases and/or access to the latest software while eliminating unexpected budget revisions.
Noncontract and Consulting Services	Cisco provides noncontract services at current time-and-materials rates. For more information contact Customer Services at 1-800-553-NETS or 1-415-326-1941.
Startup Services	
Total Implementation Services (TIS)	Cisco Total Implementation Solutions (TIS) is a portfolio of services that deliver the tools, expertise, and resources needed to install, configure, and implement Cisco equipment. TIS is intended to supplement services that resellers provide, either directly or indirectly, to their customers. Product Components: Installation, Configuration, and Implementation. For more information, see http://www.cisco.com/go/tis

For More Information

See the Partner and Reseller Support Services Web page at:
http://www.cisco.com/en/US/products/index.html (CCO login required)

Product Warranty Information

All Cisco hardware and software products are covered for a minimum of 90 days. Some products have a longer or more appropriate coverage, ranging from One-Year to Limited Lifetime warranties. Note that all Warranties are applicable to original owner only and support is subject to product end-of-life terms.

Warranty[1]	Entitlements Description
Cisco Standard 90-day Hardware Warranty, Software Warranty and License Agreement (78-5235-vvrr)	• Advance Replacement shippingwithin 10 business days from RMA date, within 90 days of original shipment from Cisco or from Cisco Reseller • 90-Day Assurance that the Media SW is delivered is defect-freeand the SW conformsto its published specifications • Guest Access to Cisco Connection Online (CCO)
90-Day Limited Hardware Warranty(78-5236-vvrr)	• Advance Replacement shippingwithin 10 business days from RMA date, within 90 days of original shipment from Cisco or from Cisco Reseller • 90-Day Assurance that the Media SW is delivered is defect-freeand the SW conformsto its published specifications • Guest Access to Cisco Connection Online (CCO)
One-Year Limited Hardware Warranty (78-10747-vvrr)	• Advance Replacement shippingwithin 10 business days from RMA date withinOne Year of original shipment from Cisco or from Cisco Reseller • 90-Day Assurance that the Media SW is delivered is defect-freeand the SW conformsto its published specifications • Guest Access to Cisco Connection Online (CCO)
Limited Lifetime Hardware Warranty (78-6310-vvrr)	• Advance Replacement shippingwithin 10 business days from RMA date during supported life of the product, starting original ship date from Cisco or Cisco reseller. (fan and power supply warranty limited to 5 years from ship-date) • 90-Day Assurance that the Media SW is delivered is defect-freeand the SW conformsto its published specifications • Guest Access to Cisco Connection Online (CCO)
End-User Software License Agreement and Software Warranty (78-3621-vvrr)	• 90-Day Assurance that the Media SW is delivered is defect-freeand the SW conformsto its published specifications • End User License Agreement terms • Guest Access to Cisco Connection Online (CCO)
5-Years Limited Hardware and 1-Year Limited Software Warranty (78-13712-vvrr)	• Replacementshipping within 15 business days from RTF date within 5 years from the original ship date from Cisco or Cisco reseller • One-Year SW support includes availability of bug fixes and maintenance releases • Cisco TAC 24x7 support for P1/P2 cases for Five years • Guest Access to Cisco Connection Online (CCO)

[1] "vv" and "rr" suffixes of the warranty document numbers represent the revision and version numbers respectively.

For More Information

See the Web site:
http://www.cisco.com/en/US/products/prod_warranties_listing.html

Cisco Capital Financing

Cisco Systems Capital offers a variety of financing and equipment leasing alternatives, both short term and long term, to customers and partners in the United States, Canada, Europe, Asia, Australia, and Latin America. Cisco Capital's financial solutions offer customers the ability to acquire new technologies or refresh existing equipment through flexible, easy-to-use programs.

For More Information

See the Cisco Systems Capital Web site: **http://www.cisco.com/go/CiscoCapital**
Within the United States, call 800 730-4090.

Cisco Authorized Refurbished Equipment (US and Canada Only)

Customers looking for used Cisco equipment can now be assured of the quality and support they come to expect from new Cisco products, through the Cisco Authorized Refurbished Equipment program. Cisco Authorized Refurbished Equipment gives customers a price competitive alternative to buying uncertified and unlicensed products off the secondary market. All equipment sold through this program is labeled "Refurbished by Cisco Systems," indicating that the product is Cisco tested, refurbished, authorized, and supported. The program is limited to certain countries, so interested customers should check with their local Cisco account manager of Cisco authorized reseller for availability.

For More Information

End Users/Customers:
cisco.com/en/US/ordering/or6/or17/order_refurbished_equipment_program_description.html
Resellers: **http://www.cisco.com/go/refurb** (click on "Refurbished Products")

Cisco Services

Cisco Services offers a wide range of services and support to customers, partners and resellers. Through a suite of support services Cisco enables you to improve the overall efficiency of your network operations and network performance, while benefiting from the broad range of Cisco engineering knowledge and experience base, leading practices and innovative, web-based tools.

Cisco Advanced Services (AS) is a comprehensive suite of professional engineering support offerings of Cisco networking solutions delivering the highest levels of availability, quality of service, and security for your specific network needs to realize business return on investment through high performance networking and communications applications enablement. Cisco Technical Support Services (TSS) offer leading-edge services to improve customer productivity, protect customer investment, and maximize operational efficiency. Cisco TSS solutions provide access to highly skilled engineers with technical expertise on multiple disciplines of technology. In addition, Cisco TSS provides you with the online tools and resources, software support and hardware replacement options to address your challenges and provide rapid problem resolution. Key support tools and knowledge provide your staff with the ability to avoid problems, maximize network utility, and expedite problem resolution.

For More Information

Technical Support Services:
http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/serv_group_home.html
Advanced Services:
http://www.cisco.com/en/US/products/svcs/ps11/serv_category_home.html

CHAPTER 1

Routers

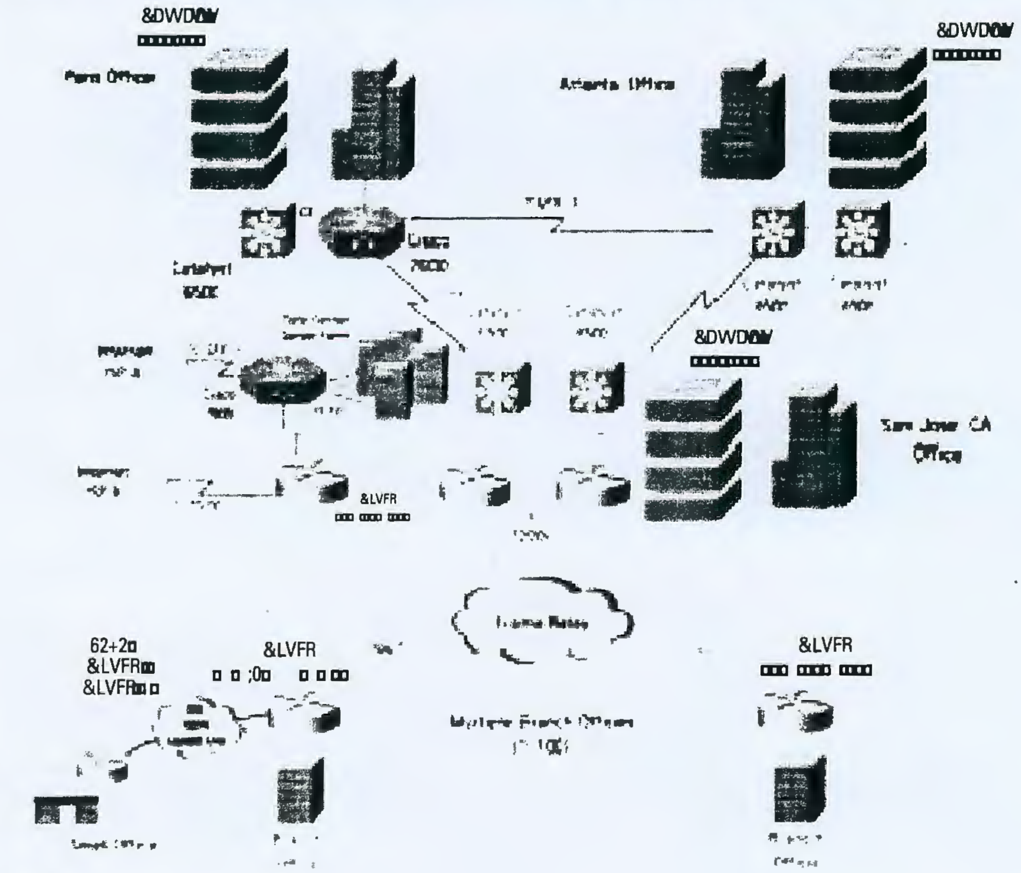
Routers at a Glance

Product	Features	Page
Cisco IOS® Software	See the Chapter 9—CiscoIOS Software and Network Management foran overview of Cisco IOS Software	9-4
Cisco SOHO Series Secure Broadband Routers	Ethernet, ADSL, ADSL over ISDN, and G.SHDSL Routers for Small Office and Home Ofices • Integrated securty of Cisco IOS Software with Stateful Inspection Firewall and software-based 3DES encryption • Easy setup and deployment using Cisco Router Web Set Up Tool (CRWS) • Offers many local and remote debug and troubleshooting features in Cisco IOS Software	1-8
Cisco 800 Series Router	Ethernet, ADSL, ADSL over ISDN, G.SHDSL, ISDN, and serial routers for small remote offices and teleworkers • 1-port Ethernet, 1-port ADSL, ADSL over ISDN or G.SHDSL or 1-port BRI (optional NT1), 1-port serial WAN • 4-port Ethernet hub or 10/100 swithch on most models and 2 analog telephone ports on ISDN models and 4 analog voice ports on 827-4V • Advanced securty features including statefulinspection firewall and hardware assisted encryption (830 series) • Toll quality voice with VoIP (Cisco 827-4V) • Dial back up and out-of-band management (Cisco 830 series)	1-9
Cisco 1700 Series Router	Flexible, secure, modular access routers • 1-port autosensing 10/100 Fast Ethernet LAN • Modular slots support a wide variety of WAN and voice interface cards • Supports secure Internet, intranet,and extranet access as well as new WAN applications including VPNs, integrated voice/data (VoIP), and broadband services • VLAN Capabilty • Supports up to three Ethernet connectionswith 1FE and 2 ENET WICs	1-11
Cisco 2500 Series Router	Fixed-port configuration access servers • The Cisco AS2509-RJ/AS2511-RJ access/terminal servers provide Ethernet LAN connectivity and enable 8 or 16 (respectively) users/devices via async connections • Ideal for low-density analog telephone lne dial access applications via external modems	1-14
Cisco 2600 Series Router	Modular multiservice router • Single or dual LAN (Ethernet, 10/100 Mbps Ethernet, Token Ring and mixed Ethernet options) • Wide variety of interface support, including integrated 16-port switching, high-density analog and digital, voice, Cisco IOS Firewall and VPN, async and sync serial, ISDN, Fractional and channelized T1/E1, Ethemet, analog modems, ADSL, G.SHDSL, switching integration, and ATM support • Shares WAN interface cards and network modules with Cisco 1700, 3600 and 3700 series • Cisco 2610XM, 2620XM, and 2650XM models offer the features of Cisco 2600 with more default memory, capacity, performance and FE support on all models.	1-16
Cisco 3600 Series Router	Modular multiservice high-densty access router • 2-, 4-, and 6-slot models • Wide variety of media support including: high density analog and digital voice, Cisco IOS Firewall and VPN, integrated 16-port switching, ADSL, and G.SHDSL, async and sync serial, BRI and PRI ISDN, channelized T1/E1, Ethernet, Fast Ethernet, Token Ring, digital and analog modems, and ATM • Digital and analog voice/fax over IP or Frame Relay or ATM • The Cisco 3640 is no longer orderable. Customers are encouraged to migrate to the Cisco 3700 Series Routers. On an interim basis we have made available the Cisco3640A as an alternative for customers with configurations not available on the Cisco3700.	1-22

Product	Features	Page
Cisco 3700 Series Router	Modular multiservice high-density access router • Enable higher levels of application and service integration in enterprise branch offices in a small form factor – Supports integrated firewall, intrusion detection, and VPN capabilities and offloads processing to on-board Advanced Integration Module (AIM) – Combines flexible routing and low density switching in a single platform with new 16 and 36-port EtherSwitch module – Delivers internal in-line power for the EtherSwitch ports for a single platform Branch Office IP Telephony and Voice Gateway – Conserves WAN bandwidth with Content Engine module to combine intellgent caching, content routing and management – Higher performance enables scalable deployment of multiple, concurrent applications • Wide variety of interface support, including integrated 36 and 16-port switching, high-density analog and digital, voice, Cisco IOS Firewall/IDS and VPN, Fractional and channelized T1/E1 and DS-3, Ethernet, Gigabit Ethernet and ADSL. • Shares WAN interface cards and network modules with Cisco 1700, 2600/2600XM, and 3600 series	1-26
Cisco 7100 Series VPN Router	Large branch and central site VPN router, for a dedicated site-to-site VPN solution See Chapter 5—VPN and Security for information on the Cisco 7100 Series VPN Routers	5-11
Cisco 7200 Series Router	WAN-edge router providing intelligent services, modularity, high performance, investment protection, and scalability in a small form factor • Modular 3 RU Chassis • 4- or 6-slot models and choice of system processors for up to 1 Mpps performance • Wide variety of LAN and WAN options, including Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, serial, ISDN, HSSI, ATM, Packet over SONET, DPT/RPR	1-31
Cisco 7300 Series	Network Edge router with high perfomance IP services delivered at optical speeds for service providers and enterprise networks • Compact and modular 4 rack unit chassis—4 slots • High performance connectivity—T3 through OC48/STM16 with 3.5 Mpps performance • Built-in Gigabit Ethernet connectivity • Multiprotocol routing: IP, IPX, AppleTalk, DLSw • Compact size, high availability and optimal cooling	1-35
Cisco 7400 Series Router	Highest performance 1 rack unit router in the industry, with a stackable architecture that is designed for service provider and enterprise networks • One port adapter slot, two built-in 10/100/GE Ethernet ports, and a broad range of WAN media interfaces from DS0 to OC3 (40+ port adapters) common with Cisco 7x00-series port adapters • High-density broadband aggregation • Managed CPE for service provider demarcation point • Gigabit Ethernet to Gigabit Ethernet IP services applications platform	1-38
Cisco 7500 Series	High-end services-enabled core and WAN aggregation router for enterprise and service provider applications • 5-, 7-, and 13-slot models • 1-, 2-, or 4-bus models offering 1, 2, or 4 Gbps backplanes • Wide variety of LAN and WAN options including Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, serial, ISDN, HSSI, ATM, and Packet over SONET	1-40
Cisco 7600 Series	Service provider and high-end enterprise-class router delivering optical WAN and Metropolitan Area Network services with high-touch IP services at the network edge. • Consolidated LAN/WAN/MAN in a single platform • Scalable backplane bandwidth from 32 Gbps to 256 Gbps and performance from 15 Mpps to 30 Mpps • High-volume aggregation of Ethernet traffic (server farms) • Wide range of WAN/MAN interfaces from NxDS0, T1, T3 to OC-48 with line rate services • Ideal for Internet data center, metropolitan aggregation, WAN edge aggregation, and enterprise core applications • Also supports Catalyst 6000 series line cards	1-45
Cisco 10000 Series	Service provider-class edge services router • High-Performance IP, MPLS, and Broadband Services — The Cisco 10000 Series enables service providers to deploy revenue-generating services without worrying about performance degradation • Carrier-Class High Availability — With its carrier-class high availability, the Cisco 10000 Series minimizes costly network outages and maximizing end-customer satisfaction • Application Integration — The Cisco 10000 Series leverages service providers' current investments by enabling leased line and broadband aggregation features on a single platform • Application Flexibility — The Cisco 10000 Series has a broad range of channelized, clear channel, ATM and LAN interfaces. Physical interface speeds from E1/T1 up to OC-48c/STM-16c	1-47

Product	Features	Page
Cisco 10700 Series	Service provider-class metro edge services router • Optimized building block for the next generation metro Ethernet/IP access networks • Equipped with either (24) 10/100 or 4 GbE and 8 FE ports for customer access and OC-48c/STM-16c dynamic packet transport/resilient packet ring (DPT/RPR) technology or Packet Over SONET (POS) for metro optical connectivity • Powered by Cisco IOS 12.0S software and the parallel express forwarding (PXF) architecture • Cost-effective, reliable, high-performance platform supporting full suite of IP/MPLS features and services found in Cisco Internet Routers • With DPT/RPR architecture, enables optimal fiber connectivity as well as features such as IP class of service, VoIP, L2 VPN (EoMPLS and L2TPv3) and L3 VPN (MPLS) services	1-49
Cisco 12000 Series	Premier high-end routing portfolio for service provider backbone and high-speed edge applications. With its unique, modular distributed system architecture, the Cisco 12000 Series Router, is the industry choice for building Carrier IP/MPLS networks with its portfolio of 10Gbps systems and interfaces: • Seven chassis options that fit your scaling and real estate requirements offering the only complete solution for small to large POPs; backbone or edge. • The only platforms supporting backbone—or edge-optimized line cards in the same chassis, maximize the value of line-rate edge applicatons with 10G uplinks, and sustained line-rate performance as they scale to maximum capacity. • Proven investment protection with simple, field upgrades to higher switching capacities. • The only complete priority packet delivery solution set—the industry's only IP QoS implementation that uniquely enables premium real time IP services such as VoIP and video. • Extensive portfolio of line cards offering leading edge technologies (POS, ATM, DPT/RPR, GbE/FE), support a wide range of networking speeds (from DS1 to OC-192c/STM-64c). • The industry's only high-end router proven (via independent lab testing) to maintain customer connections and network traffic with zero packet loss despite a route processor failure.	1-51
Cisco SN 5400 Series Storage Router	Enables direct access to storage systems anywhere on an IP network. Enables SCSI over IP (iSCSI); the first storage implementation based on IP standards. • Cisco SN 5428: Migrates DAS (Direct Attached Storage) environments to SAN (Storage Area Networks) for small / medium businesses and enterprise workgroups. This is a full function Fibre Channel switch that adds iSCSI, providing very low price per port networked storage configurations	1-55

Sample Routing Solutions Overview—WAN & Internet Data Center



AA

Cisco Routers Port Matrix

	SOHO Series	800 Series	1700 Series	2600 Series	3600 Series	3700 Series	7100 Series	7200 Series	7300 Series	7400 Series	7500 Series	7600 Series	10000 Series	10720 Series	12000 Series
Fixed Ports Only	X	X													
Fixed & Modular Ports			X	X	X[1]	X	X		X			X			
Modular Ports Only					X[2]			X		X	X		X	X	X
LAN Ports															
10-MB Ethernet	X	X	X	X	X	X	X	X		X	X	X		X	
10-MB Ethernet (fiber)					X		X	X		X	X	X			
100-MB Ethernet			X	X	X	X	X	X		X	X	X		X	X
100-MB Ethernet (fiber)					X		X	X		X	X	X	X	X	X
10/100-MB Eth	X	X	X	X	X	X	X	X						X	
Token Ring				X	X	X	X				X				
FDDI/CDDI											X				
ATM	X	X		X	X	X		X		X	X	X	X		
Gigabit Ethernet						X	X	X	X	X	X	X	X	X	X
WAN Ports															
Sync Serial		X	X	X	X	X		X		X	X	X			
Sync Serial w/ CSU			X	X	X	X							X		
ISDN BRI (S/T)		X	X	X	X	X	X	X		X	X				
ISDN BRI (U)		X	X	X	X	X	X	X		X	X				
ISDN PRI/Ch T1				X	X	X	X	X		X	X	X			
ISDN PRI w/ CSU				X	X	X		X		X	X	X			
Async			X	X	X	X									
Analog/POTS		X		X	X	X									
Integrated Modems				X	X	X									
Integrated Modem WICs			X	X	X	X									
HSSI				X[3]	X	X	X	X		X	X	X			
DS3				X	X	X	X	X		X	X	X	X		X
ATM OC-3				X[3]	X	X	X	X		X	X	X	X		X
ATM OC-12								X		X	X	X	X		X
ATM				X	X	X		X		X	X	X	X		X
ATM - T1/E1				X	X	X	X	X		X	X	X			
POS OC-x/STM-x							X	X	X	X	X	X	X		X
DPT/RPR OC-12/STM-4								X			X				X
DPT/RPR OC-48/STM-16												X	X	X	X
DPT/RPR OC-192/STM-64															X
ADSL	X	X	X	X	X	X									
ADSL over ISDN	X	X													
G.SHDSL	X	X	X	X		X									
IDSL		X	X	X		X									
DPT								X			X		X	X	X

	SOHO Series	800 Series	1700 Series	2600 Series	3600 Series	3700 Series	7100 Series	7200 Series	7300 Series	7400 Series	7500 Series	7600 Series	10000 Series	10720 Series	12000 Series
Voice Ports															
Analog		X	X	X	X	X									
Digital			X	X	X	X		X		X	X	X			
Integrated Switching															
Integrated 16-port Switching				X	X	X									
Integrated 36-port Switching					X[1]	X									
Inline Power				X[4]	X[4]	X									
Content Acceleration and Delivery															
Content Engine				X	X	X									
Security/VPN															
Encryption Advanced Integration Modules				X	X[1]	X									
Encryption Network Module					X[2]	X									

1. Cisco 3660 only
2. Cisco 3620 and 3640
3. Supported on the 2691 only
4. Requires external power source

Memory Information for Routers

Router	Memory Type	Slots	Default Memory	Max Memory	Default Configuration (Notes)
SOHO 78	Flash	1	8 MB	8 MB	No Upgradeable Memory
	DRAM	1	16 MB	16 MB	
SOHO 90	Flash	1	8 MB	8 MB	No Upgradeable Memory
	DRAM	1	32 MB	32 MB	
801, 802, 803, and 804	Flash	1	8 MB	12 MB	4MB on board and4MB or 8MB Mini flash card
	DRAM	1	4 MB	12 MB	4MB onboard and 4MB or 8MB DIMM module
805	Flash	1	4 MB	12 MB	
	DRAM	1	8 MB (On board)	16 MB	4MB On board + 4MB Mini Flash
811 and 813	Flash	1	8MB	12MB	4MB On board + 4MB or 8MB Mini Flash
	DRAM	1	8MB	16MB	8MB on board and4MB or 8MB DIMM Module
827-4V, 828	Flash	1	8 MB	16 MB	8MB On board + 4MB Mini Flash
	DRAM	1	16 MB (827-4V: 24 MB, 806: 32MB)	32 MB	16MB Onboard and 4MB or 8MB or 16MB DIMM Module
831, 836, 837	Flash	1	8 MB	24 MB	
	DRAM	1	32 MB	48 MB	
1721	Flash	1	16 MB	16 MB	Uses Mini Flash
	DRAM	1	32 MB (On board)	48 MB	
1751	Flash	1	16 MB	48 MB	
	DRAM	1	32 MB	96 MB	
1760	Flash	1	16 MB	64 MB	
	DRAM	1	32 MB	96 MB	
2500 Series	Flash	2	8 MB	16 MB	Slot 0 = 8 MB
	DRAM	1	4 MB	16 MB	
2600 Series	Flash (261xXM, 262xXM, 265xXM)	1	16 MB	48 MB	16 MB on Mother Board; Slot 0 = 32 MB
	Flash (261x)	1	8 MB	16 MB	Slot 0 = 8 MB
	Flash (262x,265x)	1	8 MB	32 MB	Slot 0 = 8 MB
	Flash (2691)	2	32 MB	128 MB	Slot 0 = 32 MB
	DRAM (261XM, 262xXM)	2	32 MB	128 MB	Slot 0 = 32 MB; Slot 1 = empty
	DRAM (265xXM)	2	64 MB	128 MB	Slot 0 = 64 MB; Slot 1 = empty
	DRAM (261x, 262x)	2	32 MB	64 MB	Slot 0 = 32 MB; Slot 1 = empty
	DRAM (265x)	2	32 MB	128 MB	Slot 0 = 32 MB; Slot 1 = empty
	DRAM (2691)	2	64 MB	256 MB	Slot 0 = 64 MB; Slot 1 = empty
3620 and 3640	Flash (PCMCIA)	2	0	32 MB	
	Flash (SIMM)	2	16 MB	32 MB	Slot 0 = 8 MB
	DRAM	4	32 MB	64 MB (3620) 128 MB (3640)	Slot 0 = 16 MB; Slot 1 = 16 MB
3660	Flash (PCMCIA)	2	0	32 MB	
	Flash (SIMM)	2	16 MB	64 MB	
	SDRAM	2	32 MB	256 MB	
3700	Flash (Internal)	1	32 MB	128 MB	
	Flash (External)	1	0 MB	32-128 MB	
	DRAM (SoDIMM)	2	128 MB	256 MB	Slot 0 = 128 MB
7100 Series	Flash (PCMCIA)	2	48 MB	110 MB	Slot 0 = 48 MB
	System SDRAM	2	64 MB	256 MB	Slot 0 = 64 MB
	Packet SDRAM		64 MB	64 MB	
7200 Series	Flash (PCMCIA)	2	20 MB	128 MB	
	Flash (non-volatile, fixed config)		128 KB	128 KB	
	Flash (C7200-IO-FE bootflash)	1	4 MB	4 MB	
	Flash (C7200-IO-2FE, C7200-IO-GE/E bootflash)	1	4 or 8 MB	4 or 8 MB	
	DRAM (NPE-225)	1	128 MB	256 MB	Slot 0 = 128 MB DIMM
	DRAM (NPE-300)	4	32+128 MB	32+256 MB	Slot 0 = 32 MB DIMM, Slot 2 = 128 MB DIMM
	DRAM (NPE-400)	1	128 MB	512 MB	Slot 0 = 128 MB SoDIMMs
	DRAM (NSE-1)	1	128 MB	256 MB	Slot 0 = 128 MB DIMM
	DRAM (NPE-G1)	1	256 MB	1 GB	Slot 0 = 128 MB SoDIMM, Slot 2 = 128 MB SoDIMM
7300 Series	Flash (CFM)	1	64 MB	128 MB	
	DRAM	1	128 MB	512 MB	

			Default		Default
Router	Memory Type	Slots	Memory	Max Memory	Configuration (Notes)
7400 Series	Flash (PCMCIA)	2	64 MB	128 MB	
	DRAM (NSE-1) BB	1	256 MB	512 MB	
	DRAM (NSE-1) CP	1	128 MB	512 MB	
7500 Series	Flash (PCMCIA) RSP2, RSP4+	1	16 MB	20 MB	
	Flash (PCMCIA) RSP8	2	20 MB	40 MB	
	Flash (PCMCIA) RSP16	1	48 MB	128 MB	
	Flash (SIMM)	1	8 MB	8 MB	
	DRAM (RSP2)	4	32 MB	128 MB	
	DRAM (RSP4+, RSP8)	2	64 MB	256 MB	
	DRAM (RSP16)	2	128 MB	1 GB	
	DRAM (VIP2-40)	1	32 MB	64 MB	
	DRAM (VIP2-50)	1	32 MB	128 MB	
	DRAM (VIP4-50/80)	1	64 MB	256 MB	
	DRAM (VIP6-80)	1	64 MB	256 MB	
7600 Series	Flash (PCMCIA)	1	16MB	20 MB	
	DRAM (Sup 2)	1	128MB	512 MB	
	DRAM (MSFC2)	1	128MB	512 MB	
	DRAM (PFC2)	1	128MB	256 MB	
10000 Series	Flash (PCMCIA)	2	48 MB	128 MB	1 x 48MB ships as default; 128MB is optional
	Flash (Internal)	1	32 MB	32 MB	
	Shared (PRE-1)	1	128 MB	128 MB	
	DRAM (PRE-1)	1	512 MB	512 MB	
10700 Series	Flash (Internal)	1	32 MB	64 MB	Maximum memory is configured with No Option
	SDRAM RP	1	256 MB	256 MB	
	Packet Buffer	1	64 MB	64 MB	
12000 Series	Flash (PCMCIA)	2	20 MB	20 MB	
	DRAM (GRP-B)	1/2	128 MB	512 MB	Route Memory
	SDRAM (PRP-1)	1/2	512 MB	1 GB	Route Memory
	DRAM (Line Cards)	1/2	128-256 MB	256-512 MB	Route Memory (line card dependent)
	SDRAM (Line Cards)	1/2	128-256 MB	256-512 MB	Packet Memory (line card dependent)
	Shared (PRE-2)	1	128 MB	128 MB	
	DRAM (PRE-2)	1	512 MB	512 MB	

Cisco SOHO Series Ethernet, ADSL over ISDN, ADSL and G.SHDSL Routers

The Cisco SOHOseries provides an affordable, secure, multi-user access solution to small office/home office (SOHO) customers while reducing deployment and operational costs for service providers. Through the power of Cisco IOS software technology, the Cisco SOHO 91 Ethernet to Ethernet Router, the SOHO 96 ADSL over ISDN, the SOHO 97 ADSL and SOHO 78 G.SHDSL routers provide superior manageability and reliability.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco SOHO 91	• Ethernet WAN port for use with an external DSL or cable modem with 4-port 10/100 switch, stateful firewall and software based encryption
Cisco SOHO 96	• ADSL modem for use of ADSL over ISDN with 4-port 10/100 switch, stateful firewall and software based encryption
Cisco SOHO 97	• ADSL modem for ADSL over POTS with 4-port 10/100 switch, stateful fiewall and software based encryption
Cisco SOHO 78	• 4-port Ethernet Hub and 1G.SHDSL port with firewall security and Cisco IOS manageabilty and reliability

Key Features

- Integrated security of Cisco IOS Software with Stateful Inspection Firewall and software-based 3DES encryption (no encryption on the SOHO 78)
- Easy setup and deployment using Cisco Router Web Set Up Tool (CRWS)
- Offers many local and remote debug and troubleshooting features in Cisco IOS Software

Competitive Products

- 3Com: OfficeConnect 810
- Alcatel: Speed Touch Pro Router
- Cayman: 3220H
- Efficient: 5861, 5660
- Lucent: CellPipe 50A
- Netopia: R6100, 4533
- Westel: Wirespeed 36R566
- Zyxel: 641, 782
- Nokia: MW1352
- Linksys: Etherfast models

Specifications

Feature	SOHO 91	SOHO 96	SOHO 97	SOHO 78
Fixed LAN Ports	4-port 10/100 Switch	4-port 10/100 Switch	4-port 10/100 Switch	4-port Ethernet (10BASE-T)
Fixed WAN Ports	1-port Ethernet (connects to external DSL or cable modem	1-port ADSL over ISDN	1-port ADSL over POTS	1-port G.SHDSL
Flash Memory	8 MB	8 MB	8 MB	8 MB
DRAM Memory	32 MB	32 MB	32 MB	16 MB
Dimensions (HxWxD)	2.0 x 9.7 x 8.5 in.	2.0 x 9.7 x 8.5 in.	2.0 x 9.7 x 8.5 in.	2.0 x 9.9 x 8.3 in. (5.1 x 25.2 x 21.1 cm)

For More Information

See the Cisco SOHO Web site: **http://www.cisco.com/go/soho90**

Cisco 800 Series

The Cisco 800 series router provides enhanced network security and proven reliability through Cisco IOS software, for small offices and telecommuters. It connects users to the Internet or to a corporate LAN via one ADSL, ADSL over ISDN, G.SHDSL, IDSL, ISDN, or serial connection (up to 512 Kbps), or with an Ethernet WAN port connected to an external broadband modem.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 800 Series	• Companies who Cisco IOS-based networks who want to add telecommuters • Service providers who offer value-added services to small offices • VARs who are familiar with Cisco IOS software and want to profitably service small office customers • Ethernet LAN ports and variety of WAN connectivity, including: ISDN BRI, Frame Relay, ADSL, G.SHDSL, async dialup (see Specificationsfor details)

Key Features

- Fixed configuration support for several types of WAN connections
- Standard security with ACLs, PAT/NAT, PAP/CHAP, MS-CHAP, Lock and Key, and Generic Routing Encapsulation (GRE) tunneling
- Enhanced security with stateful inspection firewall, IPSec encryption (hardware based on Cisco 830s and AES encryption on Cisco 830s)
- Toll quality voice with VoIP on Cisco 827-4V
- Integrated 4-port 10/100 Ethernet Switch on Cisco 830 series
- Bandwidth optimization features such as compression, Bandwidth-on-Demand, Dial-on-Demand, Always-On-Dynamic-ISDN (AODI), and X.25 over D channel (Cisco 801- 804)
- Support for CAPI applications in the European market

Competitive Products

- 3Com: Office Connect Remote 511/521
- Alcatel: Speed Touch Pro Routers
- Ascend: Pipeline 75/85
- Efficient: 5861 / 5660
- Intel: Express 8100
- Netopia: R3100, R6100, 4533
- Nortel/Bay: Nautica 250
- Nokia: MW1352
- Zyxel: 782
- Linksys: Etherfast

Specifications

Cisco 801, 802, 803, 804, 805, 811 and 813

Feature	801	802	803	804	811	813
Fixed LAN Port Connections	1-port Ethernet (10BASE-T)	1-port Ethernet (10BASE-T)	4-port Ethernet hub (10BASE-T)	4-port Ethernet hub (10BASE-T)	1-port Ethernet (10BASE-T)	4-port Ethernet hub (10BASE-T)
Fixed WAN Port Connections	1-port ISDN BRI (S/T)	1-port ISDN BRI (U) NT-1	1-port ISDN BRI (S/T) 2 analog ports	1-port ISDN BRI (U) NT-1 2 analog ports	1-port ISDN BRI S/T and 1-port ISDN BRI (U) NT-1	1-port ISDN BRI S/T and 1-port ISDN BRI (U) NT-1 2 analog ports
Flash Memory	8MB (default) 12 MB (max)	8MB (default) 12 MB (max)	8MB (default) 12 MB (max)	8MB (default) 12 MB (max)	4MB (default) 12MB (max)	8MB (default) 12MB (max)
DRAM Memory	4MB (default) 12MB (max)	4MB (default) 12MB (max)	4MB (default) 12MB (max)	4MB (default) 12MB (max)	8MB (default) 16MB (max)	8MB (default) 16MB (max)
Dimensions (HxWxD)	2.0 x 9.9 x 8.3 in. (5.1 x 25.2 x 21.1 cm)	Same as Cisco 801	Same as Cisco 801	Same as Cisco 801	Same as Cisco 801	Same as Cisco 801

Cisco 800 Series (805, 836, 827-4V, 828, 836, 837)

Feature	805	827-4V	828	831	836	837
Fixed LAN Port Connections	1-port Ethemet (10BASE-T)	1-port Ethemet (10BASE-T)	4-port Ethemet hub (10BASE-T)	4-port Ethemet (10BASE-T)	1-port Ethemet (10BASE-T)	4-port Ethemet (10BASE-T)
Fixed WAN Port Connections	1-port Serial (Up to 512 KBPS)	1-port ADSL	1-port G.SHDSL	1-port Ethernet	1-port ADSL-over-ISDN, 1-port ISDN S/T	1-port ADSL over POTS
Flash Memory	4MB (default) 12MB (max)	8MB (default) 16MB (max)	8MB (default) 16MB (max)	8MB (default) 24MB (max)	8MB (default) 24MB (max)	8MB (default) 24MB (max)
DRAM Memory	8MB (default) 16MB (max)	24MB (default) 32MB (max)	16MB (default) 32MB (max)	32MB (default) 48MB (max)	32MB (default) 48MB (max)	32MB (default) 48MB (max)
Dimensions (HxWxD)	2.0 x 9.9 x 8.3 in. (5.1 x 25.2 x 21.1 cm)	Same as Cisco 805	Same as Cisco 805	2.0 x 9.7 x 8.5 in.	2.0 x 9.7 x 8.5 in.	2.0 x 9.7 x 8.5 in.

Selected Part Numbers and Ordering Information[1]

Cisco 800 Series Routers	
CISCO801	1-port 10BASE-T, 1-port BRI (S/T), IP s/w
CISCO802	1-port 10BASE-T, 1-port BRI (U) w/ NT-1, IP s/w
CISCO803	4-port 10BASE-T hub, 1-port BRI (S/T), 2-port POTS, IP s/w
CISCO804	4-port 10BASE-T hub, 1-port BRI (U) w/ NT-1, 2-port POTS, IP s/w
CISCO805	1-port 10BASE-T, 1-port serial, IP s/w
CISCO801-CAPI	ISDN/Ethernet Router with one-user CAPI license
CISCO803-CAPI	ISDN/Ethernet Router with one-user CAPI license, 4-port hub
CISCO827-4V	1-port ADSL, 1-port 10BASE-T, 4 ports FXS, IP/Voice s/w
CISCO828	1-port G.SHDSL, 4-port 10BASE-T hub, IP s/w
CISCO831-K9 USD 649.00	Cisco 831 Ethernet Router
CISCO836-K9	Cisco 836 ADSL over ISDN Router
CISCO837-K9	Cisco 837 ADSL Router
Cisco 800 Series CD Feature Packs	
CD08-BHL-12.0.7XV=	Cisco 800 Series IP/IPX/FW Plus IPSec 56
CD08-BP-12.07.XV=	Cisco 800 Series IP/IPX/Plus
CD800-5CAPI=	CAPI 5 User CD
CD08-IC-12.0.5T=	Cisco 800 Series Internet DSL
CD08-ICHL-12.0.5T=	Cisco 800 Series Internet DSL FW IPSec56
CD08-IBHL-12.0.5T=	Cisco 800 Series Internet DSL IPX FW IPSec56
Cisco 800 Series Memory Options	
MEM800-4F=	Cisco 800 Series, 4 MB Flash Mini-Card
MEM800-8F=	Cisco 800 Series, 8 MB Flash Mini-Card
MEM800-4D=	Cisco 800 Series, 4 MB DRAM DIMM
MEM800-8D=	Cisco 800 Series, 8 MB DRAM DIMM
MEM820-8U16F	Cisco 820 Flash upgrade 8Mbyte-16Mbyte
MEM820-16U20D	Cisco 820 DRAM upgrade 16Mbyte-20Mbyte (16Mbyte-24Mbyte & 16Mbyte-32Mbyte also available)
MEM820-24U32D	Cisco 820 DRAM 24Mbyte upgrade to 32 Mbytes
Cisco 800 Series Accessories	
PWR-8xx-WW1=	Cisco 8xx Series, AC Power Supply Spare
Cisco 800 Series Basic Maintenance	
CON-SNT-PKG1	Cisco 800 Series SMARTnet Maintenance (8x5xNBD)

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco 800 Series Web site: **http://www.cisco.com/go/800**

Cisco 1700 Series

The Cisco 1700 series modular access routers are designed to provide a cost-effective integrated access platform for small and medium-sized businesses and enterprise small branch offices. These Cisco IOS-based routers deliver high-speed network access, comprehensive security features, and multiservice data/voice/video/fax integration to meet the most demanding business requirements. Within the Cisco 1700 series, Cisco 1710 security access routers work with existing broadband modems to provide advanced routing and security functionality, Cisco 1721 modular access routers provide flexible, high-performance data access, and Cisco 1751 and Cisco 1760 modular access routers are optimized for both voice and data traffic, providing a simple and cost-effective path to multi-service networking—today or in the future.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 1710	• Advanced routing and security functionalityin one device when connecting to the Internet using a broadband modem • Hardware-assisted 3DES VPN encryption at fullT1/E1 speeds
Cisco 1721	• Secure data-only access solution that adapts to customers' evolving network requirements • Support for data applicationsincluding VPNs and broadband access services • A broad array of WAN services supported, including Frame Relay, leased line, ADSL, G.SHDSL, ISDN BRI, X.25, SMDS and more • IPSec 3DES VPN encryption at full T1/E1 speeds • IEEE 802.1Q VLAN Support
Cisco 1751	All the above, plus: • Analog and digital voice support in a desk-top form factor • 3 modular slots for WAN and Voice interface cards
Cisco 1760	All the above, plus: • 19" rackmount form factor • 4 slots with 2 WIC/VIC and 2 VIC slots • Multiservice analog anddigital voice support • Highest performance multi-service router in the Cisco 1700 family • Higher density analog and digital voice support than Cisco 1751

Key Features

- Support for up to 4 serial interfaces or 2 ISDN BRI; 1 autosensing 10/100 Mbps Fast Ethernet LAN connection; 1 auxiliary (AUX) port for dial-up management or low-speed asynchronous connections (up to 112.5 kbps)
- Flexibility—Cisco 1700 Series supports a diverse set of WAN and Voice Interface Cards that are shared with the 1600 (WAN only), 2600/2600XM, and 3600 series routers enabling field upgradeability to evolve with the needs of growing businesses
- Integrated Device—Cisco 1700 series combines WAN routing, VPN and multiservice access in a single device
- Expansion Slot—Supports optional hardware VPN module for wire-speed IPSec 3DES encryption and can enable future technologies (VPN Module standard on Cisco 1710)
- Integrated Security—The 1700 series supports context-based access control for dynamic firewall filtering, denial-of-service detection and prevention, Java blocking, real-time alerts, Intrusion Detection System (IDS), and encryption.
- IEEE 802.1Q VLAN Support

Specifications

Feature	Cisco 1710	Cisco 1721	Cisco 1751/1751-V	Cisco 1760/1760-V
Fixed LAN Ports (connections)	1-port autosensing 10/100 Mbps Ethernet	1-port autosensing 10/100 Mbps Ethernet	1-port autosensing 10/100 Mbps Ethernet	1-port autosensing10/100 Mbps Ethernet
Fixed WAN Ports	1-port 10BASE-T Ethernet for broadband modem	None	None	None
Modular Slots	None	2 WAN slots	3 slots (2 WAN or Voice slots and 1 Voice-only slot)	4 Slots (2 WAN or Voice slots and 2 Voice-only slots)
WAN Interface Card (WIC) Modules	None	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Voice Interface Cards (VIC) Modules	None	None	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Flash Memory	16 MB Flash (default/max)	16 MB (default); 16 MB (max)	1751 base model: 16 MB (default); 16 MB (max) 1751-V multiservice ready configuration: 32 MB (default); 32 MB (max)	1760 base model: 16-MB Flash Memory (on board) 64-MB (max) 1760-V: 32-MB Flash 64-MB (max)
DRAM Memory	64 MB	32 MB (default);96 MB (max)	1751 base model: 32 MB (default); 96 MB (max) 1751-V multiservice-ready configuration:64 MB (default); 96 MB (max)	1760 base model:32 MB (default)96 MB (max)1760-V:64 MB (default)96 MB (max)
Dimensions (HxWxD)	3.1 x 11.2 x 8.7 in.	3.1 x 11.2 x 8.7 in.	4.0 x 11.2 x 8.7 in.	1.7 x 17.5 x 12.8 in.

Cisco IOS Software and Memory Requirements[1]

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required	DRAM Memory Required
CD17-C- 12.x	IP only IP/ADSL	12.1 Mainline	4 MB 8 MB	16 MB 20 MB
CD17-CH-12.x	IP/FW	12.1 Mainline	4 MB	20 MB
CD17-CP-12.x	IP Plus	12.1 Mainline	4 MB	20 MB
CD17-CHK2-12.x	IP/FW Plus IPSEC 3DES	12.1 Mainline	8 MB	32 MB
CD17-CVP-12.x	IP/Voice Plus	12.1 Mainline	8 MB	24 MB
CD17-CHV-12.x	IP/FW/Voice Plus	12.1 Mainline	8 MB	24 MB
CD17-CHVK2-12.x	IP/FW/Voice Plus IPSEC 3DES	12.1 Mainline	8 MB	24 MB
CD17-C- 12.x	IP only	12.1T	4 MB	16 MB
CD17-CH-12.x	IP/FW	12.1T	4 MB	20 MB
CD17-CP-12.x	IP Plus	12.1T	8 MB	24 MB
CD17-CK2-12.x	IP Plus IPSEC 3DES	12.1T	8 MB	32 MB
CD17-CHK2-12.x	IP/FW Plus IPSEC 3DES	12.1T	8 MB	32 MB
CD17-CVP-12.x	IP/Voice Plus	12.1T	8 MB	32 MB
CD17-CHV-12.x	IP/FW/Voice Plus	12.1T	8 MB	32 MB
CD17-CVK2-12.x	IP/Voice Plus IPSEC 3DES	12.1T	8 MB	32 MB
CD17-CHVK2-12.x	IP/FW/Voice Plus IPSEC 3DES	12.1T	8 MB	32 MB

[1] For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information." For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

Selected Part Numbers and Ordering Information[1]

Cisco 1700 Series Modular Access Routers

CISCO1760	10/100 Modular Router w/ 2WIC/VIC,2VIC slots,19 inch Chassis
CISCO1760-ADSL	10/100 BaseT Modular Router w/ADSL WIC, IP/ADSL
CISCO1760-SHDSL	10/100 BaseT Modular G.SHDSL Router, 19 inch Chassis
CISCO1760-VPN/K9	1760 VPN Bundle with VPN Module, 48MB DRAM, IP Plus/FW/3DES
CISCO1760-VPN/K9-A	1760 VPN Bun. w/ADSL WIC, VPN Module, 48MB DRAM, IP+/FW/3DES
CISCO1760-V	10/100 Modular Router w/Voice IP/VOICE Plus, 19 inch Chassis
CISCO1751	10/100 Modular Router w/ 3 slots, IOS IP, 16F/32D
CISCO1751-V	10/100 Modular Router w/Voice, IOS IP/VOICE Plus, 32F/64D
CISCO1751-VPN/K9	1751 VPN Bundle with VPN Module, 48MB DRAM, IP Plus/FW/3DES
CISCO1751-VPN/K9-A	1751 VPN Bun. w/ADSL WIC, VPN Module, 48MB DRAM, IP+/FW/3DES
CISCO1721-ADSL	10/100 BaseT Modular ADSL Router, IP/DSL

CISCO1721	10/100BaseT Modular Router w/2 WAN slots, 16M Flash/32M DRAM
CISCO1721-VPN/K9	1721 VPN Bundle with VPN Module, 48MB DRAM, IP Plus/FW/3DES
CISCO1721-VPN/K9-A	1721 VPN Bun. w/ADSL WIC, VPN Module, 48MB DRAM, IP+/FW/3DES
CISCO1721-SHDSL	10/100 BaseT Modular G.SHDSL Router, IP/DSL
CISCO1710-VPN-M/K9	Dual-Ethernet SecurityAccess Router, VPN Module, IP/3DES/FW

Cisco 1751 Software Feature Packs for Cisco IOS Release 12.1.(5)YB

CD17-C-12.1.5=	IP
CD17-C-12.1.5=	IP ADSL
CD17-C7P-12.1.5=	IP Plus ADSL
CD17-C7K2-12.1.5=	IP Plus IPSec 3DES ADSL
CD17-CH-12.1.5=	IP/FW/IDS
CD17-B-12.1.5=	IP/IPX
CD17-B7HP-12.1.5=	IP/IPX/FW/IDS Plus ADSL
CD17-C7HK2-12.1.5=	IP/FW/IDS Plus IPSec 3DES ADSL
CD17-Q7HK2-12.1.5=	IP/IPX/AT/IBM/FW/IDS Plus IPSec 3DES
CD17-C7VP-12.1.5=	IP/Voice Plus
CD17-C7VP-12.1.5=	IP/Voice Plus ADSL
CD17-C7HV-12.1.5=	IP/Voice/FW/IDS Plus ADSL
CD17-C7VK2-12.1.5=	IP/Voice Plus IPSec 3DES ADSL
CD17-C7HVK2-12.1.5=	IP/Voice/FW/IDS Plus IPSec 3DES ADSL
CD17-Q7HVK2-12.1.5=	IP/IPX/AT/IBM/FW/IDS/Voice Plus IPSec 3DES

Cisco 1700 Series Memory Options

MEM-1700-4MFC=	Cisco 1700 Series, 4 MB Mini-Flash Card
MEM-1700-8MFC=	Cisco 1700 Series, 8 MB Mini-Flash Card
MEM-1700-16D=	Cisco 1700 Series, 16 MB DRAM DIMM
MEM-1700-32D=	Cisco 1700 Series, 32 MB DRAM DIMM
MEM-1700-64D+	Cisco 1700 Series, 64 MB DRAM DIMM

Cisco 1700 Series WAN Interface Cards (WICs)

WIC-1T	1-port Serial WAN Interface Card
WIC-2T	2-port Serial WAN Interface Card
WIC-2A/S	2-port Async/Sync Serial WAN Interface Card
WIC-1B-S/T	1-port BRI (S/T) WAN Interface Card (dialand leased line)
WIC-1B-U	1-port BRI w/ NT-1 WAN Interface Card (dialand leased line)
WIC-1DSU-56K4	1-port 4-Wire 56/64 Kbps w/ (DSU/CSU) WAN Interface Card
WIC-1DSU-T1	1-port T1/Fr T1 w/ (DSU/CSU) WAN Interface Card
WIC-1ADSL=	1-port ADSL WAN Interface Card
WIC-1SHDSL	1-port G.SHDSL WAN Interface Card
WIC-1ENET=	1-port Ethernet Interface Card

Cisco 1751/1760 Voice Interface Cards

VIC-2FXS	2-port Voice Interface Card FXS
VIC-4FXS	4-port Voice Interface Card FXS
VIC-2FXO	2-port Voice Interface Card FXO
VIC-2E/M	2-port Voice Interface Card E&M
VIC-2FXO-EU	2-port Voice Interface Card FXO for Europe
VIC-2FXO-M	32-port Voice Interface Card FXO for Australia
VIC-2BRI-NT/TE	2-port Voice Interface Card—BR (NT & TE)
VIC-2FXO-M1	2-port FXO for U.S. with batteryreversal
VIC-2FXO-M2	2-port FXO for Europe with batteryreversal
VIC-2DID	2-port FXO analog DID

Cisco 1700 Multiflex Voice / WAN interface Cards

VWIC-1MFT-E1	1-Port RJ-48 Multiflex Trunk - E1
VWIC-1MFT-E1=	1-Port RJ-48 Multiflex Trunk - E1
VWIC-1MFT-G703	1-Port RJ-48 Multiflex Trunk - G.703
VWIC-1MFT-G703=	1-Port RJ-48 Multiflex Trunk - G.703
VWIC-2MFT-E1	2-Port RJ-48 Multiflex Trunk - E1
VWIC-2MFT-E1=	2-Port RJ-48 Multiflex Trunk - E1
VWIC-2MFT-E1-DI	2-Port RJ-48 Multiflex Trunk - E1 With Drop and Insert
VWIC-2MFT-E1-DI=	2-Port RJ-48 Multiflex Trunk - E1 With Drop and Insert
VWIC-2MFT-G703	2-Port RJ-48 Multiflex Trunk - G.703
VWIC-2MFT-G703=	2-Port RJ-48 Multiflex Trunk - G.703
VWIC-1MFT-T1	1-Port RJ-48 Multiflex Trunk - T1
VWIC-1MFT-T1=	1-Port RJ-48 Multiflex Trunk - T1
VWIC-2MFT-T1-DI	2-Port RJ-48 Multiflex Trunk - T1 With Drop and Insert
VWIC-2MFT-T1-DI=	2-Port RJ-48 Multiflex Trunk - T1 With Drop and Insert
VWIC-2MFT-T1	2-Port RJ-48 Multiflex Trunk - T1
VWIC-2MFT-T1=	2-Port RJ-48 Multiflex Trunk - T1

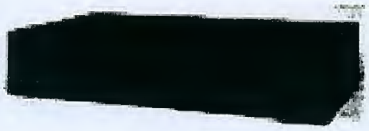
Cisco 1700 Module Options	
MOD1700-VPN	Cisco 1700 Series VPN Module
Cisco 1700 Spares and Accessories	
PWR-1700-WW1=	Cisco 1700 AC Power Supply—worldwide
PVDM-256K-4=	4-Channel Packet Voice/Fax DSP Module for the 1751
PVDM-256K-8=	8-Channel Packet Voice/Fax DSP Module for the 1751
PVDM-256K-12=	12-Channel Packet Voice/Fax DSP Module for the 1751
PVDM-256K-16=	16-Channel Packet Voice/Fax DSP Module for the 1751
PVDM-256K-20=	20-Channel Packet Voice/Fax DSP Module for the 1751
Cisco 1700 Series Basic Maintenance	
CON-SNT-PKG4	Cisco 1751-V SMARTnet Maintenance
CON-SNT-PKG3	Cisco 1751 and 1710-VPN-M/K9 SMARTnet Maintenance
CON-SNT-PKG2	Cisco 1720 and 1720-ADSL SMARTnet Maintenance

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco 1700 Series Web site: **http://www.cisco.com/go/1700**

Cisco 2500 Series



The Cisco 2500 series router has served for years as the most deployed and popular branch office router in the world, and provides low cost routing functionality for data-only applications (no voice support). There are currently two access servers to choose from, 8 or 16 asynchronous ports, each with 1 Ethernet port, for aggregating multiple network elements to provide a single Telnet access point (telemetry application)—or for attaching 8 to 16 external analog or digital modems in environments where T1/E1 digital circuits are not available, but multiple dial-up telephone lines can be leveraged for low cost remote access.

For higher performance requirements, where a wider variety of WAN/LAN interfaces are needed, as well as voice support, refer to Cisco 2600/2600XM/3600 or 1700 series routers.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco AS2509-RJ and AS2511-RJ	• Data-only network requirement • An access server combining a terminal server, protocol translator, console port aggregator, and a router in a single device • One Ethernet LAN and dual serial ports • 8 or 16 asynchronous serial ports with RJ-11 jacks, ideal for attaching 8 to 16 external modems

Key Features

- Proven technology with a full suite of Cisco IOS Software
- Setup with Cisco ConfigMaker, a free tool for configuring a network of routers
- With CiscoWorks for Windows, allows remote management and maintenance from a central location

Specifications

Feature	Cisco AS2509-RJ	Cisco AS2511-RJ
Throughput Performance (pps)	3-5 Kpps (dependingon configuration)	3-5 Kpps (depending on configuration)
Memory	8-MB dual Flash bank option (default) 16 MB (max) 16 MB DRAM (default)	Same as Cisco AS2509-RJ
Power Supply	AC, with optional DC or redundant power supply	Same as Cisco AS2509-RJ
Fixed LAN Ports	1-port Ethernet	1-port Ethernet
Fixed WAN Ports	1-port sync serial 8-port async	1-port sync serial 16-port async
Dimensions (H x W x D)	1.75 x 17.5 x 10.56 in.	1.75 x 17.5 x 10.56 in.

Cisco IOS Software and Memory Requirements

To run the Cisco IOS software Feature Packs, you need the amount of memory shown in the following table:

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required[2]	DRAM Memory Required
CD25-C-12.0=	IP only	12.0(10)	8 MB	4 MB
		12.0(7)T	8 MB	6 MB
CD25-CP-12.0=	IP Plus	12.0(10)	8 MB	6 MB
		12.0(7)T	16 MB	8 MB
CD25-CHL-12.0=	IP/FW Plus IPSEC 56	12.0(10)	16 MB	8 MB
		12.0(7)T	16 MB	10 MB
CD25-B-12.0=	IP/IPX/AT/DEC	12.0(10)	8 MB	6 MB
		12.0(7)T	**16 MB**	6 MB
CD25-BP-12.0=	IP/IPX/AT/DEC Plus	12.0(10)	16 MB	6 MB
		12.0(7)T	16 MB	8 MB
CD25-AP-12.0=	Enterprise Plus	12.0(10)	16 MB	6 MB
		12.0(7)T	16 MB	10 MB

[1] For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

[2] Bold numbers indicate that more memory than the default amount is needed to run the Feature Pack.

Selected Part Numbers and Ordering Information[1]

Cisco 2500 Series Access Router Chassis	
CISCO2509-CH	1-port Ethernet AUI, 2-port Serial, 8-port Async Serial, IP s/q
AS2509-RJ-CH	1-port Ethernet AUI (RJ-45), 1-port Serial, 8-port Async Serial, IP s/w
CISCO2511-CH	1-port Ethernet AUI, 2-port Serial, 16-port Async Serial, IP s/w
AS2511-RJ-CH	1-port Ethernet AUI (RJ-45), 1-port Serial, 16-port Async Serial, IP s/w
Cisco 2500 Series Memory Options	
MEM-1X4F=	Cisco 2500 Series, 4 MB Flash Upgrade
MEM-1X8F=	Cisco 2500 Series, 8 MB Flash Upgrade
MEM-1X8D=	Cisco 2500 Series, 8 MB DRAM Upgrade
MEM-1X16D=	Cisco 2500 Series, 16 MB DRAM Upgrade
Cisco 2500 Series Accessories	
ACS-2500RM-19=	Cisco 2500 Series, Rack-Mount Kit, 19 Inches
ACS-2500RM-24=	Cisco 2500 Series, Rack-Mount Kit, 24 Inches
ACS-2500ASYN=	Cisco 2500 AUX/Console Part Cable Kit
ACS-2500RPS=	Cisco 2500 Series, RPS Field Upgrade
Cisco 2500 Series Basic Maintenance	
CON-SNT-PKG4	Packaged SMARTnet (8 x5 x NBD) for the Cisco AS2509 and AS2511

For More Information

See the Cisco 2500 Series Web site: **http://www.cisco.com/go/2500**

Cisco 2600 Series

The Cisco 2600 series is an award-winning family of modular multiservice access routers, providing flexible LAN and WAN configurations, multiple security options, voice/data integration, and a range of high performance processors. This range of features make the Cisco 2600 series the ideal branch-office router for today's and tomorrow's customer requirements.

The Cisco 2600 series family of modular routers include the Cisco 2600XM models, the Cisco 2691 and the Cisco 2612 token ring router. These new models deliver extended performance, higher density, enhanced security performance and increased concurrent application support to meet the growing demands of branch offices.

The Cisco 2600XM models are based on the classic Cisco 2600 platform architecture, and extend the performance by as much as 33%. They also increase default platform memory and provide increases in memory capacity at the same price as their Cisco 2600 predecessor.

The highest performing router in the Cisco 2600 family that extends the density of emerging branch office applications, is the Cisco 2691 offering almost twice the performance of the Cisco 2650XM platform while leveraging the same modules from other Cisco 2600, Cisco 3600 and Cisco 3700 Series routers. Compared to the Cisco 2600XM models, the new Cisco 2691 is designed to offer a higher degree of versatility, providing greater throughput for higher density WAN applications, support for high speed interfaces and increased performance to handle new services.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 2691	• Enterprises wanting a higherlevel of performance for a broadened range of concurrent remote office applications including unparalleled voice/data integraton, Virtual Private Network (VPN) performance, increased bandwidth to suppot voice and video applications and the delivery of Web-based applications
Cisco 2600XM Series	• Enterprises consideringthe Cisco 2600 for branch office applicationsshould now regard the Cisco 2600XM as the preferential platform for delivering high performing, flexible solutions to branch and remote offices. • High Performance 10/100 Dual Ethernet Router with 3 WIC Slots, 1 NM
Cisco 2651XM	• High performance Dual10/100 Modular Router with CiscoIOS IP
Cisco 2650XM	• High performance 10/100 Modular Router with Cisco IOS IP
Cisco 2621XM	• Mid Performance Dual10/100 Ethernet Router with Cisco IOS IP
Cisco 2620XM	• Mid Performance 10/100 Ethemet Router with Cisco IOS IP
Cisco 2611XM	• Dual 10/100 Ethemet Router with Cisco IOS IP
Cisco 2610XM	• 10/100 Ethernet Router with Cisco IOS IP
Cisco 2612	• One Token Ring port and one Ethernet port formixed LANs and migrating from Token Ring to Ethemet

Key Features

- Integration/manageability—Lowers cost of ownership and improves ease of remote management, providing integrated "branch-in-a-box" networking that combines CSU/DSUs, multiplexors, modems, voice/data gateways, ISDN NT1s, firewalls, VPNs, encryption, and compression devices
- Multiservice voice/data networks—Reduces phone/fax costs between offices; using Cisco IOS software QoS features (such as RSVP, WFQ, CAR, and RED), voice/fax traffic is digitized and encapsulated in Frame Relay or IP packets and consolidated with data traffic

- Enterprise/Provider class solution—Meets the requirements of multiservice enterprises and their managed service CPE providers with high reliability features, multiple WAN connections, and the ability to migrate from data- only to TDM voice and data to packetized voice and data infrastructure
- High-density analog/fax network modules provide the ability to directly connect PSTN and legacy telephony equipment to existing Cisco 2600 and 3600 routers
- An EtherSwitch network module for the Cisco 2600/3600 series with 16 ports of 10/100 Ethernet and one optional 1000BaseT (Gigabit Ethernet) connection, providing a fully integrated Layer 2 (L2) switch with the capability to support both Line Power to Cisco IP phones and current Aironet 802.11 wireless base stations (with the addition of an external power supply). This provides a single box solution for branch offices deploying converged IP telephony, extending data, voice and video by delivering IP routing, Ethernet switching, fixed wireless solutions and voice gateway capabilities
- A wide range of Virtual Private Network modules (VPN) optimize the Cisco 2600 Series platforms for virtual private networks (VPNs) and delivers a rich integrated package of routing, firewall, intrusion-detection, and VPN functions
- The introduction of the WIC-ADSL and WIC-1SHDSL, offers business-class broadband service with scalable performance, flexibility, and security for branch and regional offices
- Content Networking Integration and Branch-Office Routing with router-integrated content-delivery system that combines intelligent caching, content routing and management with robust branch-office routing, WAN bandwidth for branch IP services such as voice over IP (VoIP)

Competitive Products

- 3Com: SuperStack II NETBuilder SI and PathbuilderS400
- Intel/Shiva: LanRover Family
- Motorola: Vanguard 645x/643x
- Nortel/Bay: Advanced Remote Node (ARN), Passport 4400 series
- FutureWei/Quidway®: R2630/31E
- Tasman: 2004, 1400

Specifications

Feature	2610/11XM	2620/21XM	2650/51XM	2691
Performance	Up to 20Kpps	Up to 30Kpps	Up to 40Kpps	Up to 70Kpps
Flash Memory (Default/Max)	16MB/48MB	16MB/48MB	16MB/48MB	32MB/128MB (Compact Flash)
System Memory (Default/Max)	32MB/128MB	32MB/128MB	64MB/128MB	64MB/256MB
Integrated WIC Slots	2	2	2	3
Onboard AIM Slot	1	1	1	2
Minimum Cisco IOS Release	12.1(14) mainline, 12.2(12) mainline, 12.2(8)T1or later	12.1(14) mainline, 12.2(12) mainline, 12.2(8)T1or later	12.1(14) mainline, 12.2(12) mainline, 12.2(8)T1or later	12.2(8)T1 or later
Onboard LAN Ports	1 to 2 10/100 FE ports	1 to 2 10/100 FE ports	1 to 2 10/100 FE ports	2 10/100 FE ports
Rack Mounting	Yes, 19" and 23" options	Yes, 19" and 23" options	Yes, 19" and 23" options	Yes, 19" and 23" options
Wall Mounting	Yes	Yes	Yes	No

Cisco IOS Software and Memory Requirements[1]

Most Cisco IOS software CD feature packs for the Cisco 2600 series include several selected Cisco IOS releases. To run the latest Cisco IOS Software Feature Packs with version 12.0(7)XK, you need, at a minimum, the amount of memory shown in the following table. Some configurations will require more than the recommended minimum.

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required	DRAM Memory Required
Cisco 2612				
CD26-C-12.0.7=	IP only	12.0(7)XK1	8 MB	24 MB
CD26-CP-12.0.7=	IP Plus	12.0(7)XK1	8 MB	40 MB
CD26-CH-12.0.7=	IP/Firewall	12.0(7)XK1	8 MB	32 MB
CD26-CHL-12.0.7=	IP/Firewall Plus IPSec 56	12.0(7)XK1	16 MB	48 MB
CD26-CHK2-12.0.7=	IP/Firewall Plus IPSec 3DES	12.0(7)XK1	16 MB	48 MB
CD26-CK2-12.0.7=	IP Plus IPSec 3DES	12.0(7)XK1	16 MB	40 MB
CD26-CL-12.0.7=	IP Plus IPSec 56	12.0(7)XK1	16 MB	40 MB
CD26-B-12.0.7=	IP/IPX/AT/DEC	12.0(7)XK1	8 MB	32 MB
CD26-BP-12.0.7=	IP/IPX/AT/DEC Plus	12.0(7)XK1	16 MB	40 MB
CD26-BHP-12.0.7=	IP/IPX/AT/DEC/Firewall Plus	12.0(7)XK1	16 MB	48 MB
CD26-AP-12.0.7=	Enterprise Plus	12.0(7)XK1	16 MB	48 MB
CD26-AL-12.0.7=	Enterprise Plus IPSec 56	12.0(7)XK1	16 MB	48 MB
CD26-AHK2-12.0.7=	Enterprise/Firewall Plus IPSec 3DES	12.0(7)XK1	16 MB	48 MB
CD26-AHL-12.0.7=	Enterprise/Firewall Plus IPSec 56	12.0(7)XK1	16 MB	48 MB
CD26-AK2-12.0.7=	Enterprise Plus IPSec 3DES	12.0(7)XK1	16 MB	48 MB
CD26-E-12.0.7=	Remote Access Server	12.0(7)XK1	8 MB	24 MB

[1] For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information." For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

Selected Part Numbers and Ordering Information[1]

Cisco 2600/2600XM Series Router Chassis	
CISCO2610XM	10/100 Ethernet Router w/Cisco IOS IP
CISCO2610XM-DC	10/100 Ethernet Router w/ Cisco IOS IP - DC
CISCO2610XM-RPS	10/100 Ethernet Router w/ Cisco IOS IP - use w/ ext RPS
CISCO2611XM	Dual 10/100 Ethernet Router w/ Cisco IOS IP
CISCO2611XM-DC	Dual 10/100 Ethernet Router w/ CiscoIOS IP - DC
CISCO2611XM-RPS	Dual 10/100 Ethernet Router w/ Cisco IOS IP - use w/ ext RPS
CISCO2620XM	Mid Performance 10/100 Ethernet Router with Cisco IOS IP
CISCO2620XM-DC	Mid Performance10/100 Ethernet Router w/Cisco IOS IP-DC
CISCO2620XM-RPS	Mid Performance 10/100 Ethernet Rout w/Cisco IOS IP-RPS ADPT
CISCO2621XM	Mid Performance Dual 10/100 Ethernet Router w/Cisco IOS IP
CISCO2621XM-DC	Mid Performance Dual10/100 Ethernet Rout w/Cisco IOS IP-DC
CISCO2621XM-RPS	Mid Performance Dual 10/100 Ethernet Rout w/IOS IP-RPS ADPT
CISCO2650XM	High Performance 10/100 Modular Router w/Cisco IOS IP
CISCO2650XM-DC	High Performance 10/100 Modular Rout w/CiscoIOS IP-DC NEBs
CISCO2650XM-RPS	High Performance 10/100 Modular Rout w/CiscoIOS IP-RPS ADPT
CISCO2651XM	High Performance Dual 10/100 Modular Rout with CiscoIOS IP
CISCO2651XM-DC	High Performance Dual 10/100 Modular Rout w/IP-DC NEB
CISCO2651XM-RPS	High Performance Dual 10/100 Mod Rout w/IP-RPS ADPT
CISCO2691	High Performance 10/100 Dual Eth Router w/3 WIC Slots,1 NM
CISCO2612	1-port 10BASE-T, 1-port TR, 1 network module slot, 1 AIM slot, 2 WIC slots, IP s/w
CISCO2612-DC	1-port 10BASE-T, 1-port TR, 1 network module slot, 1 AIM slot, 2 WIC slots, DC Power Supply, IP s/w
CISCO2612-RPS	1-port 10BASE-T, 1-port TR, 1 network module slot, 1 AIM slot, 2 WIC slots, RPS adapter, IP s/w
Cisco 2600 Series Voice Gateway Bundles	
CISCO2651XM-V	CISCO2651XM, AIM-VOICE-30, IOS IP Plus, 96D/32F
CISCO2651XM-V-SRST	CISCO2651XM, FL-SRST-MEDIUM, AIM-VOICE-30, IOS IP Plus, 96D/32F

Cisco 2600 Series VPN Bundles

CVPN2600FIPS/KIT=	KIT (Instructions, labels) to configued 2600 for FIPS
C2651XM-2FE/VPN/K9	2651XM/VPN Bundle, AIM-VPN/EP/2FE/IOS FW/IPSec 3 DES, 96DRAM
C2621XM-2FE/VPN/K9	2621XM/VPN Bundle, AIM-VPN/EP/2FE/IOS FW/IPSec 3 DES, 96DRAM
C2611XM-2FE/VPN/K9	2611XM/VPN Bundle, AIM-VPN/EP/2FE/IOS FW/IPSec 3 DES, 96DRAM
C2691-VPN/K9	2691 VPN Bundle,AIM-VPN/EPII, Plus IOS/FW/IPSEC3DES

Cisco 2600 Series DSL Bundles

CISCO2651XM-ADSL	2651XM-ADSL Bundle, WIC-1ADSL, 2FE, IP Plus, 32F/96DRAM
CISCO2621XM-ADSL	2621XM-ADSL Bundle, WIC-1ADSL, 2FE, IP Plus, 32F/96DRAM
CISCO2611XM-ADSL	2611XM-ADSL Bundle, WIC-1ADSL, 2FE, IP Plus, 32F/96DRAM
CISCO2651XM-SHDSL	2651XM-SHDSL Bundle, WIC-1SHDSL, 2FE, IP Plus, 32F/96DRAM
CISCO2621XM-SHDSL	2621XM-SHDSL Bundle, WIC-1SHDSL, 2FE, IP Plus, 32F/96DRAM
CISCO2611XM-SHDSL	2611XM-SHDSL Bundle, WIC-1SHDSL, 2FE, IP Plus, 32F/96DRAM

Cisco 2600/2600XM Series LAN Modules

NM-1E=	1-port 10BASE-T network module
NM-4E=	4-port 10BASE-T network module

Cisco 2600/2600XM and 3600 Series WAN Interface Cards (WICs)

WIC-1B-S/T=	1-port BRI (S/T) WAN Interface Card (Dialand Leased Line)
WIC-1B-U-V2	1-port BRI (U) w/NT-1 WAN Interface Card (Dialand Leased Line)
WIC-1DSU-56K4=	1-port Serial W/ 4-Wire 56/64Kbps DSU/CSU WAN Interface Card
WIC-1DSU-T1=	1-port Serial w/ FrT1/T1 DSU/CSU WAN Interface Card
WIC-1T=	1-port Serial WAN Interface Card
WIC-2T=	2-port Serial WAN Interface Card
WIC-2A/S=	2-port Async/Sync Serial WAN Interface Card
WIC-1ADSL=	1-port ADSL WAN Interface Card
WIC-1SHDSL=	1-port G.SHDSL WAN Interface Card
WIC-1AM=	1-port Analog Modem WAN Interface Card
WIC-2AM=	2-port Analog Modem WAN Interface Card

Cisco 2600/2600XM and 3600 Series Multiflex Voice and WAN Interface Cards[2]

VWIC-1MFT-T1=	1-port RJ-48 Multiflex TrunkT1
VWIC-2MFT-T1=	2-port RJ-48 Multiflex Trunk—T1
VWIC-2MFT-T1-DI=	2-port RJ-48 Multiflex Trunk—T1 With Drop and Insert
VWIC-1MFT-E1=	1-port RJ-48 Multiflex Trunk—E1
VWIC-1MFT-G703=	1-port RJ-48 Multiflex Trunk-G.703
VWIC-2MFT-E1=	2-port RJ-48 Multiflex Trunk—E1
VWIC-2MFT-G703=	2-port RJ-48 Multiflex Trunk-G.703
VWIC-2MFT-E1-DI=	2-port RJ-48 Multiflex Trunk—E1 With Drop and Insert

Cisco 2600/2600XM and 3600 Series Voice/Fax Network Modules and Expansion Modules

NM-1V=	1-slot voice/fax network module
NM-2V=	2-slot voice/fax network module
NM-HDV-1T1-24=	1-port T1 24 channel voice/fax network module
NM-HDV-1T1-24E=	1-port T1 24 enhanced channelvoice/fax network module
NM-HDV-2T1-48=	2-port T1 48 channel voice/fax network module
NM-CE-BP-20G-K9=	Content EngineNM-Basic Perf-20GB
NM-CE-BP-40G-K9=	Content EngineNM-Basic Perf-40GB
NM-CE-BP-SCSI-K9=	Content Engine NM-Basic Perf-SCSI Adapter
NM-HDV-1E1-30=	1-port E1 30 channel voice/fax network module
NM-HDV-1E1-30E=	1-port E1 30 enhanced channelvoice/fax network module
NM-HDV-2E1-60=	2-port E1 60 channel voice/fax network module
NM-HDV=	High density voice networkmodule, spare (no T1/E1 or DSPs)
NM-HDA-4FXS=	High density analog voice/fax networkmodule with 4 FXS
EM-HDA-8FXS=	8-port FXS voice/fax expansion module
EM-HDA-4FXO=	4-port FXO voice/fax expansion module
DSP-HDA-16	16-channel DSP module for NM-HDA

Cisco 2600/2600XM and 3600 Series ATM Modules

NM-4T1-IMA=	4-port T1 ATM network module with IMA
NM-4E1-IMA=	4-port E1 ATM network module with IMA
NM-8T1-IMA=	8-port T1 ATM network module with IMA
NM-8E1-IMA=	8-port E1 ATM network module with IMA

Cisco 2600/2600XM and 3600 Series EtherSwitch Modules

NM-16ESW=	Sixteen 10BaseT/100BaseTX autosensing ports EtherSwitch
NM-16ESW-PWR=	Sixteen 10BaseT/100BaseTX autosensing ports EtherSwitch with power daughter card

Cisco 2600/2600XM and 3600 Series High-Density Voice/Fax DSP Upgrade Modules

PVDM-12=	12-channel Packet Voice/Fax DSP Module

Cisco 2600/2600XM and 3600 Series Voice Interface Cards (VICs)

VIC-2E/M=	2-port E&M Voice Interface Card
VIC-2FXO=	2-port FXO Voice Interface Card
VIC-2FXS=	2-port FXS Voice Interface Card
VIC-2DID=	2-port DID Voice/Fax Interface Card
VIC-2FXO-EU=	2-port FXO Voice InterfaceCard (for Europe)
VIC-2FXO-M3=	2-port FXO Voice Interface Card (forAustralia)
VIC-2BRI-S/T-TE=	2-port BRI (S/T user side) Voice Interface Card
VIC-2FXO-M1=	2-port Voice Interface Card—FXO w/ Reversal (for US+)
VIC-2FXO-M2=	2-port Voice Interface Card—FXO w/ Reversal (for EU)

Cisco 2600/2600XM and 3600 Series WAN Network Modules

NM-4B-S/T=	4-port BRI (S/T) networkmodule
NM-8B-S/T=	8-port BRI (S/T) networkmodule
NM-4B-U=	4-port BRI (U) w/ NT1 network module
NM-8B-U=	8-port BRI (U) w/ NT1 network module
NM-4A/S=	4-port Async/Sync Serial network module
NM-8A/S=	8-port Async/Sync Serial network module
NM-16A=	16-port Async Serial network module
NM-32A=	32-port Async Serial network module
NM-1CT1=	1-port Channelized T1/ISDN-PRI network module
NM-2CT1=	2-port Channelized T1/ISDN-PRI network module
NM-1CT1-CSU=	1-port Channelized T1/ISDN-PRI w/ CSU network module
NM-2CT1-CSU=	2-port Channelized T1/ISDN-PRI w/ CSU network module
NM-1ATM-25=	1-port ATM 25 network module

Cisco 2600/2600XM and 3600 Series Modem Network Modules

NM-8AM=	8-port Analog Modemnetwork module
NM-16AM=	16-port Analog Modem networkmodule

Cisco 2600/2600XM and 3600 Series Network Modules (International)

NM-1CE1B=	1-port Channelized E1/ISDN-PRI balanced networkmodule
NM-1CE1U=	1-port Channelized E1/ISDN-PRI unbalanced networkmodule
NM-2CE1B=	2-port Channelized E1/ISDN-PRI balanced networkmodule
NM-2CE1U=	2-port Channelized E1/ISDN-PRI unbalanced networkmodule

Cisco 2600/2600XM and 3600 Series Modem Management Technology Licenses (MMTL)[3]

MMTL-3600/2600-8=	MMTL for 8 Analog Modems
MMTL-3600/2600-16=	MMTL for 16 Analog Modems

Cisco 2600/2600XM Series Advanced Integration Modules

AIM-COMPR2=	Data Compression AIM forthe Cisco 2600/2600XM series
AIM-COMPR4=	Data Compression AIM for the Cisco 2691/3660/3700 series
AIM-VPN/BP=	DES/3DES VPN Encryption AIMfor 2600-Base Performance
AIM-ATM=	ATM SAR Only AIM
AIM-ATM-1T1=	High Performance ATM AIM/T1 Bundle AIM-ATM
AIM-ATM-1E1=	High Performance ATM AIM/E1 Bundle AIM-ATM
AIM-VPN/-EP=	DES/3DES VPN Encryption Module for 2600-Enhanced Performance
AIM-VPN/-EPII=	DES/3DES/AES VPN Encryption Module for 2691/3725
AIM-ATM-VOICE-30=	30-Channel T1/E1 Digital Voice Module
AIM-VOICE-30=	SAR and 30-Channel T1/E1 Digital Voice Module

Cisco 260/2600XM0 Series Factory Memory Options

Product Number	Product Description
MEM2691-32CF-EXT	32MB External Compact Flash Memory for the 2691
MEM2691-64CF-EXT	64MB External Cisco Flash Memory for the 2691
MEM2691-128CF-EXT	128MB External Cisco Flash Memory for 2691

Cisco 2600/2600XM Series Factory DRAM Memory Upgrades

MEM2600-32U40D	32- to 40-MB DRAM Factory Upgrade forthe Cisco 2600 Series
MEM2600-32U48D	32- to 48-MB DRAM Factory Upgrade forthe Cisco 2600 Series
MEM2600-32U64D	32- to 64-MB DRAM Factory Upgrade forthe Cisco 2600 Series
MEM2650-32U40D	32 TO 40MB DRAM Factory Upgrade for the Cisco 265x only
MEM2650-32U48D	32 TO 48MB DRAM Factory Upgrade for the Cisco 265x only
MEM2650-32U64D	32 TO 64MB DRAM Factory Upgrade for the Cisco 265x only
MEM2650-32U96D	32 TO 96MB DRAM Factory Upgrade for the Cisco 265x only
MEM2650-32U128D	32 TO 128MB DRAM Factory Upgrade forthe Cisco 265x only
MEM2600XM-32U128D	32 to 128MB DRAM factory upgrade for Cisco 261x/2xXM
MEM2600XM-32U64D	32 to 64MB DRAM factory upgrade for Cisco 261x/2xXM
MEM2600XM-32U96D	32 to 96MB DRAM factory upgrade for Cisco 261x/2xXM
MEM2600XM-64U128D	64 to 128MB DRAM factory upgrade - 265xXM/XM VPN Bundles
MEM2600XM-64U96D	64 to 96MB DRAM factory upgrade - 265xXM/XM VPN Bundles
MEM2691-64U128D	64 to 128MB DIMM DRAM factory upgrade for the Cisco 2691
MEM2691-64U192D	64 to 192MB DIMM DRAM factory upgrade for the Cisco 2691

MEM2691-64U256D	64 to 256MB DIMM DRAM factory upgrade for the Cisco 2691
Cisco 2600/2600XM Series Factory Flash Memory Upgrades	
MEM2600-8U16FS	8 to 16 MB Flash Factory Upgrade for the Cisco 2600 Series
MEM2620-8U32FS	8 TO 32MB Flash SIMM Upgrade for the Cisco262x only
MEM2650-8U32FS	8 TO 32MB Flash SIMM Upgrade for the Cisco265x only
MEM2600XM-16U32FS	16 to 32 MB Flash Factory Upgrade for the Cisco 2600XM
MEM2600XM-16U48FS	16 to 48MB Flash Factory Upgrade for the Cisco 2600XM
MEM2691-32U128CF	32 to 128MB Cisco 2691 Compact Flash factory upgrade
MEM2691-32U64CF	32 to 64MB Cisco 2691 Compact Flash factory
MEM-CE-256U512D	256MB DRAM Factory Upgrade for NM-CE-BP
Cisco 2600/2600XM Series Memory Spares	
MEM2600-8D=	8 MB DRAM DIMM for the Cisco 2600 Series
MEM2600-16D=	16 MB DRAM DIMM for the Cisco 2600 Series
MEM2600-32D=	32 MB DRAM DIMM for the Cisco 2600 Series
MEM2600-4FS=	4 MB Flash SIMM for the Cisco 2600 Series
MEM2600-8FS=	8 MB Flash SIMM for the Cisco 2600 Series
MEM2600-16FS=	16 MB Flash SIMM for the Cisco 2600 Series
MEM2620-32FSBOOT=	32MB FLASH SIMM and BOOTROM for 262x Dnly
MEM2650-32FS=	32MB Flash SIMM for the Cisco 265x only
MEM2650-8D=	8MB DRAM DIMM for the Cisco 265x only
MEM2650-16D=	16MB DRAM DIMM for the Cisco 265x only
MEM2650-32D=	32MB DRAM DIMM for the Cisco 265x only
MEM2650-64D=	64MB DRAM DIMM for the Cisco 265x only
MEM2600XM-16FS=	16MB Flash SIMM for the Cisco 2600XM
MEM2600XM-32D=	32MB DIMM DRAM for the Cisco 2600XM
MEM2600XM-32FS=	32MB Flash SIMM for the Cisco 2600XM
MEM2600XM-64D=	64MB DIMM DRAM for the Cisco 2600XM
MEM2691-128CF=	128MB Cisco 2691 Compact Flash Memory
MEM2691-128D=	128MB DIMM DRAM for the Cisco 2691
MEM2691-32CF=	32MB Cisco 2691 Compact Flash Memory
MEM2691-64CF=	64MB Cisco 2691 Compact Flash Memory
MEM2691-64D=	64MB DIMM DRAM for the Cisco 2691
MEM-CE-256D=	256MB DRAM Field Upgrade for NM-CE-BP
Cisco 2600/2600XM Series Spares - Power Supplies and Other	
PWR-2600-AC=	Cisco 2600/2600XM AC power supply spare
PWR-2600-DC=	Cisco 2600/2600XM DC power supply spare
PWR-2650-AC=	Cisco265x AC power supply spare
ACS-2600RPS=	RPS Field Upgrade for the Cisco 2600 Series
ACS-2600RM-19=	19 Inch Rack Mount Kit for the Cisco2600 series
ACS-2600RM-24=	24 Inch/23 Inch Rack Mount Kit for the Cisco 2600 Series
ACS-2600ASYN=	Auxiliary and Console Port Cable Kit for Cisco 2600 Series
ACS-2600NEBS/ETSI=	NEBS/ETSI Telco Accessory Kit for Cisco 2600
CAB-RPS-2218	RPS 22/18 Load Cable
CAB-RPS-2218=	RPS 22/18 Load Cable
CAB-RPSY-2218	RPS 22/18 Two-to-one DC Power Cable
CAB-RPSY-2218=	RPS 22/18 Two-to-one DC Power Cable
PWR600-AC-RPS-CAB	600W Redundant AC Power System With DC Power Cables
PWR600-AC-RPS-NCAB	600W Redundant AC Power System W/O DC Power Cables
BOOT-2600=	Boot ROM for Cisco 2600 Series
Cisco 2600/2600XM Series SMARTnet Maintenance	
CON-SNT-PKG5	Cisco 2600 Series Packaged SMARTnet 8x5xNBD Maintenance
Cisco 2691 Series Network Modules	
NM-1GE=	1 Port GE Network Module
NM-1T3/E3=	One port T3/E3 network module

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).
2. VoIP and VoFR require use of a Voice/Fax network module
3. Requires Plus feature pack

For More Information

See the Cisco 2600 Series Web site: **http://www.cisco.com/go/2600**

Cisco 3600 Series

The Cisco 3600 Series is a family of modular, high-performance multiservice access routers for medium and large-sized branch offices and Internet service providers. With over 100 modular interface options (shares modular interfaces with the 2600/2600XM series), the Cisco 3600 Series provides solutions for voice/data integration, virtual private networks (VPNs), dial access, and multiprotocol data routing. Using Cisco's digital and analog voice/fax network modules, the Cisco 3600 Series allows customers to consolidate voice, fax, and data traffic on a single network. Its architecture protects customers' investment in network technology and integrates the functions of several devices into a single, manageable solution. Cisco 3600 VPN and Dial Bundles are also available to also address specific VPN/security, and dial-up remote access server requirements. Customers are encouraged to migrate to the Cisco 3700 Series.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 3620	• Medium-density WAN and dialup connectivity • Medium-density LAN connectivity • Low-density Voice over Data • Low-density ATM connections • Mid-density modem-over-PRI bundles
Cisco 3640A	• High-density WAN and dialup connectivity • Medium- to high-density LAN connectivity • Mid-density Voice over Data • Low- to mid-density ATM connections • Low-density modem-over-BRI bundles • Configurations not available on the Cisco 3700
Cisco 3660	• Very high-density WAN and dialup connectivty • High-density LAN connectivity • Mid-density Voice over Data • Mid-density ATM connections • Mid- to high-density modem-over-PRI and BRI connectivity

Key Features

- Combines dial access, advanced LAN-to-LAN routing services, ATM connectivity, and multiservice integration of voice, video, and data in a single platform
- Modular, scalable design provides performance, scalability, flexibility, and investment protection
- High-density ISDN PRI capabilities
- Preconfigured BRI and PRI modem bundles available
- Support for modem-over-BRI functionality
- Integrated Cisco IOS software (base price includes IP IOS software)
- Full VPN and Firewall support
- ADSL and G.SHDSL support
- ISDN Modem backup

Specifications

Feature	Cisco 3620	Cisco 3640	Cisco 3660
Fixed Ports	None	None	1 or 2 10/100 Fast Ethernet
Network Module Slots	2	4	6
Advanced Integration Module (AIM) Slots	None	None	2
LAN/Combo Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
WAN Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620 (Hardware compression support only through AIM-COMPR4)
ATM Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Voice/Fax Network Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
WAN Interface Card (WIC) Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Multiflex Voice/WAN Interface Cards	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Voice Interface Card (VIC) Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Modem Modules	See Part Numbersand Ordering Information	Same as Cisco 3620	Same as Cisco 3620
Performance	40 kpps	50-70 kpps	100-120 kpps
Flash Memory	8 MB (default);32 MB (max)	Same as Cisco 3620	8 MB (default); 64MB (max)
DRAM Memory	32 MB (default) 64 MB (max)	32 MB (default) 128 MB (max)	32 MB SDRAM (default) 256 MB SDRAM (max)
Power Supply	AC, DC optional	AC, DC optional	Single or dual AC/DC
Dimensions (HxWxD)	1.75 x 17.5 x 13.5 in.	3.44 x 17.5 x 15 in.	8.7 x 17.5 x 11.8 in.

Cisco IOS Software and Memory Requirements[1]

To run the Cisco IOS Feature Packs, you need the following amount of memory:

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required[2]	DRAM Memory Required
Cisco 3620 and 3640				
CD36-C-12.0.7=	IP only	12.0(7)XK	8 MB	32 MB
CD36-CP-12.0.7=	IP Plus	12.0(7)XK	16 MB	48 MB
CD36-CH-12.0.7=	IP/FW	12.0(7)XK	8 MB	32 MB
CD36-CHL-12.0.7=	IP/FW Plus IPSec 56	12.0(7)XK	16 MB	64 MB
CD36-CHK2-12.0.7=	IP/FW Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB
CD36-CK2-12.0.7=	IP/ Plus IPSec 3DES	12.0(7)XK	16 MB	48 MB
CD36-CL-12.0.7=	IP Plus IPSec 56	12.0(7)XK	16 MB	48 MB
CD36-B-12.0.7=	IP/IPX/AppleTalk/DECnet	12.0(7)XK	8 MB	32 MB
CD36-BP-12.0.7=	IP/IPX/AppleTalk/DECnet Plus	12.0(7)XK	16 MB	48 MB
CD36-BHP-12.0.7=	IP/IPX/AT/DEC/FW Plus	12.0(7)XK	16 MB	64 MB
CD36-AP-12.0.7=	Enterprise Plus	12.0(7)XK	16 MB	64 MB
CD36-AL-12.0.7=	Enterprise Plus IPSec 56	12.0(7)XK	16 MB	64 MB
CD36-AHK2-12.0.7=	Enterprise/FW Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB
CD36-AHL-12.0.7=	Enterprise/FW Plus IPSec 56	12.0(7)XK	16 MB	64 MB
Cisco 3660				
CD36-C-12.0.7=	IP only	12.0(7)XK	8 MB	32 MB SDRAM
CD36-CP-12.0.7=	IP Plus	12.0(7)XK	16 MB	64 MB SDRAM
CD36-CH-12.0.7=	IP/FW	12.0(7)XK	8 MB	64 MB SDRAM
CD36-CHL-12.0.7=	IP/FW Plus IPSec 56	12.0(7)XK	16 MB	64 MB SDRAM
CD36-CHK2-12.0.7=	IP/FW Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB SDRAM
CD36-CK2-12.0.7=	IP/ Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB SDRAM
CD36-CL-12.0.7=	IP Plus IPSec 56	12.0(7)XK	16 MB	64 MB SDRAM
CD36-B-12.0.7=	IP/IPX/AppleTalk/DECnet	12.0(7)XK	8 MB	64 MB SDRAM
CD36-BP-12.0.7=	IP/IPX/AppleTalk/DECnet Plus	12.0(7)XK	16 MB	64 MB SDRAM

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required[2]	DRAM Memory Required
CD36-BHP-12.0.7=	IP/IPX/AT/DEC/FW Plus	12.0(7)XK	16 MB	64 MB SDRAM
CD36-AP-12.0.7=	Enterprise Plus	12.0(7)XK	16 MB	64 MB SDRAM
CD36-AL-12.0.7=	Enterprise Plus IPSec 56	12.0(7)XK	16 MB	64 MB SDRAM
CD36-AHK2-12.0.7=	Enterprise/FW Plus IPSec 3DES	12.0(7)XK	16 MB	64 MB SDRAM
CD36-AHL-12.0.7=	Enterprise/FW Plus IPSec 56	12.0(7)XK	16 MB	64 MB SDRAM

1. For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information". For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn
2. Bold numbers indicate that more memory than the default amount is needed to run the Feature Pack.

Selected Part Numbers and Ordering Information[1]

Cisco 3600 Series Router Chassis	
CISCO3620	2-slot Modular Router-AC Power Supply, IP s/w
CISCO3620-DC	2-slot Modular Router-DC Power Supply, IP s/w
CISCO3620-RPS	2-slot Modular Router, w/ RPS, IP s/w
CISCO3640	4-slot Modular Router-AC Power Supply, IP s/w
CISCO3640-DC	4-slot Modular Router-DC Power Supply, IP s/w
CISCO3640-RPS	4-slot Modular Router, w/ RPS, IP s/w
CISCO3661-DC	10/100 E Cisco 3660 6-slot Modular Router-DC with IP SW
CISCO3661-AC	10/100 E Cisco 3660 6-slot Modular Router-AC with IP SW
CISCO3662-DC	Dual 10/100 E Cisco 3660 6-slot Modular Router-DC with IP SW
CISCO3662-AC	Dual 10/100 E Cisco 3660 6-slot Modular Router-AC with IP SW
Cisco 3600 Series Bundles	
3640MBUNDLE-4B-S/T	3640 BRI Dial bundle. Includes 1E2W,12DM, 4 BRI-S/T, IP IOS
3640MBUNDLE-4B-U	3640 BRI Dial bundle. Includes 1E2W,12DM, 4 BRI-U, IP IOS
3640MBUNDLE-8B-S/T	3640 BRI Dial bundle. Includes 1E2W,18DM, 8 BRI-S/T, IP IOS
3640MBUNDLE-8B-U	3640 BRI Dial bundle. Includes 1E2W,18DM, 8 BRI-U, IP IOS
3620MBUNDLE-24DM	3620 PRI Dial bundle. Includes 1FE2CT1-CSU, 24DM, IP IOS
AS3640-T1-48DM	3600 Access Concentrator, 48 MICA Modems, 2 PRI/T1, Ethernet, IP IOS
AS3640-E1-60DM	3600 Access Concentrator, 60 MICA Modems, Ethernet, IP IOS,no PRI
Cisco 2600/2600XM and 3600 Series ATM Modules[2]	
Cisco 2600/2600XM and 3600 Series WAN Interface Cards (WICs)[2]	
Cisco 2600/2600XM and 3600 Series Multiflex Voice/WAN Interface Cards[2]	
Cisco 2600/2600XM and 3600 Series Voice/Fax Network Modules[2]	
Cisco 2600/2600XM and 3600 Series High-Density Voice/Fax DSP Upgrade Modules[2]	
Cisco 2600/2600XM and 3600 Series Network Modules (International)[2]	
Cisco 3600 Series LAN/Combo Network Modules	
NM-1E=	1-port 10BASE-T Network Module
NM-4E=	4-port 10BASE-T Network Module
NM-1FE-TX=	1-port 100BASE-TX Network Module
NM-1FE-FX=	1-port 100BASE-FX Network Module
NM-1E2W=	1-port 10BASE-T, 2 WIC Slots Network Module
NM-2E2W=	2-port 10BASE-T, 2 WIC Slots Network Module
NM-1E1R2W=	1-port 10BASE-T, 1-port Token Ring, 2 WIC Slots Network Module
NM-1FE1CT1=	1-port 100BASE-TX, 1-port Channelized T1/ISDN-PRI Network Module
NM-1FE1CT1-CSU=	1-port 100BASE-TX, 1-port Channelized T1/ISDN-PRI with CSU Network Module
NM-1FE1CE1B=	1-port 100BASE-TX, 1-port Channelized E1/ISDN-PRI (Balanced) Network Module
NM-1FE1CE1U=	1-port 100BASE-TX, 1-port Channelized E1/ISDN-PRI (Unbalanced) Network Module
NM-1FE2CT1=	1-port 100BASE-TX, 2-port Channelized T1/ISDN-PRI Network Module
NM-1FE2CT1-CSU=	1-port 100BASE-TX, 2-port Channelized T1/ISDN-PRI with CSU Network Module
NM-1FE2CE1B=	1-port 100BASE-TX, 2-port Channelized E1/ISDN-PRI (Balanced) Network Module
NM-1FE2CE1U=	1-port 100BASE-TX, 2-port Channelized E1/ISDN-PRI (Unbalanced) Network Module
NM-1FE2W=	1-port 10/100 Ethernet, 2 WIC Slots Network Module
NM-2FE2W=	2-port 10/100 Ethernet, 2 WIC Slots Network Module
NM-1FE1R2W=	1-port 10/100 Ethernet, 1-port Token Ring, 2 WIC Slots Network Module
NM-2W=	2 WIC Slots Network Module
Cisco 3600 Series Voice Interface (VIC) Cards	
VIC-2E/M=	2-port Voice Interface Card—E&M
VIC-2FXO=	2-port Voice Interface Card—FXO
VIC-2FXS=	2-port Voice Interface Card—FXS
VIC-2BRI-S/T-TE=	2-port Voice Interface Card—BR (S/T user side)
VIC-2DID=	2-port Voice Interface Card—Direct InwardDial (DID)
VIC-2FXO-EU=	2-port Voice Interface Card—FXO (for Europe)

Cisco 3600 Series WAN Modules

NM-4B-S/T=	4-port BRI (S/T) Module
NM-8B-S/T=	8-port BRI (S/T) Module
NM-4B-U=	4-port BRI (U) w/ NT-1 Module
NM-8B-U=	8-port BRI (U) w/ NT-1 Module
NM-4T=	4-port Serial Module
NM-4A/S=	4-port Async/Sync Serial Module
NM-8A/S=	8-port Async/Sync Serial Module
NM-16A=	16-port Async Module
NM-32A=	32-port Async Module
NM-1CT1=	1-port Channelized T1/ISDN-PRI Module
NM-1CT1-CSU=	1-port Channelized T1/ISDN-PRI w/ CSU Module
NM-2CT1=	2-port Channelized T1/ISDN-PRI Module
NM-2CT1-CSU=	2-port Channelized T1/ISDN-PRI w/ CSU Module
NM-1HSSI=	1-port HSSI Module
NM-COMPR=	Compression Module
NM-VPN/MP=	DES/3DES VPN Encryption NMfor the 3620/3640 Mid-Platform

Cisco 3660 AIM Modules

AIM-VPN/HP=	DES/3DES VPN Encryption AIMfor 3660 High Performance
AIM-COMPR4=	Data Compression AIM for the 3600 series
AIM-ATM=	ATM SAR Only ATM
AIM-ATM-VOICE-30=	30-Channel T1/E1 Digital Voice Module
AIM-VOICE-30=	SAR and 30-Channel T1/E1 Digital Voice Module

Cisco 3620/40 VPN Module

NM-VPN/MP=	DES/3DES VPN Encryption NMfor 3620/3640 Mid Performance

Cisco 3600 Series Modem Modules

NM-6DM=	6-port Digital Modem Module
NM-8AM=	8-port Analog Modem Module
NM-12DM=	12-port Digital Modem Module
NM-16AM=	16-port Analog Modem Module
NM-18DM=	18-port Digital Modem Module
NM-24DM=	24-port Digital Modem Module
NM-30DM=	30-port Digital Modem Module
MICA-6MOD=	6-port Digital Modem Module (Spare)

Cisco 3600 Series Modem Management Technology Licenses[3]

MMTL-3600-6=	Modem Management Technology License (6 modems)
MMTL-3600-12=	Modem Management Technology License (12 modems)
MMTL-3600-18=	Modem Management Technology License (18 modems)
MMTL-3600-24=	Modem Management Technology License (24 modems)
MMTL-3600-30=	Modem Management Technology License (30 modems)
MMTL-3600/2600-8=	Modem ManagementTechnology License (for 8 Analog Modems)
MMTL-3600/2600-16=	Modem ManagementTechnology License (for 16 Analog Modems)

Cisco 3600 Series Memory Options

MEM3600-8FC=	Cisco 3600 Series 8 MB Flash PCMCIA Card
MEM3600-16FC=	Cisco 3600 Series 16MB Flash Card
MEM3600-8FS=	Cisco 3600 Series 8 MB Flash
MEM3600-16FS=	Cisco 3600 Series 16 MB Flash
MEM3600-2X8FS=	Cisco 3600, 16 MB Flash (2x8 MB Flash SIMMs)
MEM3600-2X16FS=	Cisco 3600, 32 MB Flash (2x16 MB Flash SIMMs)
MEM3620-8D=	Cisco 3620, 8 MB DRAM SIMM
MEM3620-16D=	Cisco 3620, 16 MB DRAM SIMM
MEM3640-2X8D=	Cisco 3640, 16 MB DRAM (2x8 MB DRAM SIMMs)
MEM3640-2X16D=	Cisco 3640, 32 MB DRAM (2x16 MB DRAM SIMMs)
MEM3640-2X32D=	Cisco 3640, 64 MB DRAM (2x32MB DRAM SIMMs)
MEM3640-4X32D=	Cisco 3640, 128 MB DRAM (4x32MB DRAM SIMMs)
MEM3660-32D=	Cisco 3660, 32 MB SDRAM Field Upgrade
MEM3660-128D=	Cisco 3660, 128 MB SDRAM Field Upgrade
MEM3660-2X64D=	Cisco 3660, 128 MB SDRAM (2x64 MB Flash DIMMs)
MEM3660-2X128D=	Cisco 3660, 256 MB Flash (2x128 MB Flash DIMMs)
BOOT-3600=	Boot ROM Upgrade for Cisco 3600

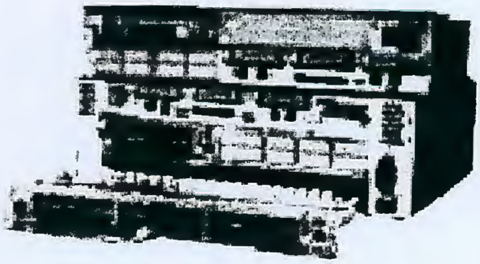
Cisco 3600 Series Accessories	
ACS-3620RM-19=	Cisco 3620—19-Inch Rack Mount Kit
ACS-3620RM-24=	Cisco 3620—24-Inch Rack Mount Kit
PWR-3620-AC	Cisco 3620—AC Power Supply
PWR-3620-DC	Cisco 3620—DC Power Supply
ACS-3620RPS=	Cisco 3620—RPS Field Upgrade
ACS-3640RM-19=	Cisco 3640—19-Inch Rack Mount Kit
ACS-3640RM-24=	Cisco 3640—24-Inch Rack Mount Kit
PWR-3640-AC	Cisco 3640—AC Power Supply
PWR-3640-DC	Cisco 3640—DC Power Supply
ACS-3640RPS=	Cisco 3640—RPS Field Upgrade
NM-BLANK-PANEL=	Blank Network Module Panel
WIC-BLANK-PANEL=	Blank WAN Interface Card Panel
ACS-3660RM-23	23 inch Rack Mount Kit for the Cisco 3660
PWR-3660-AC	AC Power Supply for Cisco 3660
PWR-3660-DC	DC Power Supply for Cisco 3660
Cisco 3600 Series Basic Packaged SMARTnet Maintenance 8x5xNBD	
CON-SNT-PKG7	Cisco 3620 Packaged SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG10	Cisco 3640 Packaged SMARTnetMaintenance 8x5xNBD
CON-SNT-PKG13	Cisco 3661 and Cisco3662 Packaged SMARTnetMaintenance 8x5xNBD

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).
2. The ATM Modules, WAN Interface Card (WIC) Modules, Multiflex Voice/WAN Interface Cards, Voice/Fax Network Modules, High-Density Voice/Fax DSP Upgrade Modules, and Network Modules (International) for the 3600 series are the same as those for the 2600 series. Please see page 1-24 for part numbers.
3. Requires Plus feature pack.

For More Information

See the Cisco 3600 Series Web site: **http://www.cisco.com/go/3600**

Cisco 3700 Series



The Cisco 3700 Series is a new line of modular routers that enable flexible and scalable deployment of new applications in an integrated branch office access platform. The Cisco 3700 Series is ideal for sites and solutions requiring the highest levels of integration at the branch for branch office IP Telephony, voice gateway, and integrated flexible routing with low-density switching solutions.Integrated security, intrusion detection, and VPN protect the network at the perimeters, while integrated caching conserves WAN bandwidth. The Cisco 3700 Series provides a consolidated service infrastructure and high service density in a compact form factor that enables the incremental incorporation of branch applications.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 3725	• New levels of branch office sewice density in a compact form factor (2RU) • Integrated Security, intrusion detection, and VPN • Integrated flexble routing and low-density switching (16-or-36 ports) • Flexible incremental and scalable migration to a voice/data converged branch office network – Compatibility with more than 90% of the world's legacy analog and digtal TDM PBXs – Survivable Remote Site Telephony (SRST) features that enable centralized call processing with local branch IP Telephony redundancy – Inline power for IP Telephony • Content Networking and Caching integrated for WAN bandwidth conservation
Cisco 3745	Same features as above plus: • New levels of branch office service density in a compact form factor (3RU) • Availability features such as redundant power, online insertion and removable components and field replaceable components • Increased performance and density

Key Features

- Optimized for multiple high density services
- Versatile High Density Service Module (HDSM) design enhances integrated services options
- Integrated connectivity options free up network module slots
- Optional features enhance availability/resiliency (3745 only): internal redundant power, hot-swappable modules, and field-serviceable components
- Optimized for Integrated IP Telephony: IP phone powered switch, high density voice gateway, flexible WAN routing, and Survivable Remote Site Telephony
- Flexible combination of analog and/or digital voice with scalable port density
- Full support for Cisco IOS voice suite of features
- Platforms performance-tuned for scaling packet voice solutions
- New integrated switching modules (16- and 36-port)
- Common user interface with Catalyst series switches
- Simplified management from a single platform for ease of configuration, deployment, and troubleshooting
- Integrated inline power for wireless access points and IP phones
- GigE connectivity

Specifications

Feature	Cisco 3725	Cisco 3745
Network Module Slots	2	4
Advanced Integration Module (AIM) Slots	2	2
WAN Interface Card (WIC) Slots	3	3
10/100 FE Ports	2	2
WAN Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
ATM Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Voice/Fax Network Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
WAN Interface Card (WIC) Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Multiflex Voice/WAN Interface Cards	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Voice Interface Card (VIC) Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Modem Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
EtherSwitch Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Performance	100 kpps	225 kpps
VPN/Security Advanced Integration Modules (AIM)	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Content Network Modules	See Part Numbers and Ordering Information	See Part Numbers and Ordering Information
Flash Memory	32 MB (default); 128 MB (max)	32 MB (default); 128 MB (max)
Flash Memory (External)	32 MB -128 MB (optional)	32 MB -128 MB (optional)
DRAM Memory	128 MB (default) 256 MB (max)	128 MB (default) 256 MB (max)
Power Supply	AC, DC optional	AC, DC optional
Dimensions (HxWxD)	3.5 x 17.25 x 14.7 in.	5.25 x 17.25 x 15 in.

Selected Part Numbers and Ordering Information[1]

Cisco 3700 SeriesModular Multiservice Access Router	
CISCO3725	2-slot Modular Multiservice Router with IP Sotware
CISCO3745	4-slot Modular Multiservice Router with IP Sotware
Serial Network Modules	
NM-4A/S	4-port async/sync serial network module
NM-8A/S	8-port async/sync serial network module
NM-1HSSI	1-port high speedserial interface module
Asynchronous Network Modules	
NM-16A	16 Async Ports network module
NM-32A	32 Async Ports network module
LAN Network Modules and Mixed-Media LAN & WAN Network Modules	
NM-2W	2 WAN Card Slot Network Module (no LAN)
NM-1FE2W	1 10/100 Ethernet2 WAN Card Slot Netwoк Module
NM-1FE1R2W	1 10/100 Ethernet 1 4/16 Token Ring 2 WAN Card Slot NM
NM-2FE2W	2 10/100 Ethernet2 WAN Card Slot Netwoк Module
NM-1FE-FX	1-port Fast Ethernet network module (10/100Base Fiber only)

Digital Packet Voice and Fax Trunk Network Modules	
NM-HDV-1T1-12	High Density Voice Network Module, with 1 VWIC-1MFT-T1 and 1 PVDM-12
NM-HDV-1E1-12	High Density Voice Network Module, with 1 VWIC-1MFT-E1 and 1 PVDM-12
NM-HDV-1E1-30	Single-port, 30-channel E1 voice/fax Network Module (supports 30 channels) of medium complexity VoCoders: G.729a/b, G.726, G.711 and fax or 12 channels of G.726, G.729, G.723.1, G.728, G.729a/b, G.711 and fax)
NM-HDV-1E1-30E	Single-port, enhanced 30-channel E1 voice/fax Network Module (supports30 channels of high and medium complexity VoCoders G.729a/b, G.726, G.729, G.728, G.723.1, G.711 and fax)
NM-HDV-2E1-60	Dual-port, 60-channel E1 voice/fax Network Module (supports 60 channels) of medium complexity VoCoders: G.729a/b, G.726,G.711 and fax or 30channels of G726, G729, G723.1, G.728, G729a/b, G711 and fax) Supportsadd/drop multiplexing (drop andinsert)
NM-HDV-1T1-24	Single-port, 24-channel T1 voice/fax Network Module (supports 24 channels of medium complexity VoCoders: G.729a/b, G.726, G.711 and fax or 12 channels of G.726, G.729, G.723.1, G.728, G.729a/b, G.711 and fax)
NM-HDV-1T1-24E	Single-port, enhanced 24-channel T1 voice/fax Network Module (supports24 channels of high and medium complexity VoCoders G.729a/b, G.726, G.729, G.728, G.723.1, G.711 and fax)
NM-HDV-2T1-48	Dual-port, 48-channel T1 voice/fax Network Module (supports 48 channels) of medium complexity VoCoders:G.729a/b,G.726,G.711 and fax or 24 channels of G726, G729, G723.1, G.728, G729a/b, G711 and fax) Supportsadd/drop multiplexing (drop andinsert)
AIM-ATM-VOICE-30	SAR and 30 Channel T1/E1 Digital Voice module
AIM-VOICE-30	30 Channel T1/E1 Digital Voice module
Analog Packet Voice and Fax Trunk Network Modules	
NM-1V	1-slot voice and fax netwok module
NM-2V	2-slot voice and fax netwok module
NM-HDA	High Density Analog Module
Voice Interface Cards	
VIC-2FXS	2-port voice interface card—FXS
VIC-2FXO	2-port voice interface card—FXO
VIC-2FXO-EU	2-port voice interface card—FXO (for Europe)
VIC-2FXO-M1	2-port voice interface card—FXO (with batteryreversal, for North America)
VIC-2FXD-M2	2-port voice interface card—FXO (with batteryreversal, for Europe)
VIC-2FXO-M3	2-port voice interface card—FXO (for Austalia)
VIC-2E/M	2-port voice interface card—E&M
VIC-2DID	2-port voice interface card—DID (Direct Inward Dial)
VIC-2BRI-S/T-TE	2-port voice interface card—BRI(Terminal side)
VIC-2BRI-NT/TE	2-port voice interface card—BRI (Network side)
ATM Network Modules	
NM-4T1-IMA	4-port T1 ATM network module with Inverse Multiplexing over ATM (IMA)
NM-4E1-IMA	4-port E1 ATM network module with IMA
NM-8T1-IMA	8-port T1 ATM network module with IMA
NM-8E1-IMA	8-port E1 ATM network module with IMA
NM-1A-T3	1-port DS3 ATM network module
NM-1A-E3	1-port E3 ATM network module
AIM-ATM	ATM cell processing module
Serial WAN Interface Cards	
WIC-1DSU-T1	One T1 CSU/DSU - Integrated
WIC-2T	2-port High Speed Serial
WIC-2-A/S	2-port Async/Sync Serial
WIC-1DSU-56K4	1-port, four-wire 56/64-Kbps with CSU/DSU
Digital Voice/WAN Interface Cards	
VWIC-1MFT-T1	1-port RJ-48 MultiFlex Trunk—T1
VWIC-2MFT-T1	2-port RJ-48 MultiFlex Trunk—T1
VWIC-2MFT-T1-DI	2-port RJ-48 MultiFlex Trunk—T1 with Drop and Insert
VWIC-1MFT-E1	1-port RJ-48 MultiFlex Trunk—E1
VWIC-2MFT-E1	2-port RJ-48 MultiFlex Trunk—E1
VWIC-2MFT-E1-DI	2-port RJ-48 MultiFlex Trunk—E1 with Drop and Insert Add not for VWICs VIC slots & WIC slots
VWIC-1MFT-G703	1-port RJ-48 MultiFlex Trunk—E1 unstructured
VWIC-2MFT-G703	2-port RJ-48 MultiFlex Trunk—E1 unstructured
ISDN WAN Interface Cards	
WIC-1B-S/T	1-port ISDN BRI
WIC-1B-U	1-port ISDN BRI with NT1

ISDN and Channelized Serial Network Modules	
NM-1CT1	1-port channelized T1/ISDN PRI network module
NM-1CT1-CSU	1-port channelized T1/ISDN PRI with CSU network module
NM-2CT1	2-port channelized T1/ISDN PRI network module
NM-2CT1-CSU	2-port channelized T1/ISDN PRI with CSU network module
NM-1CE1B	1-port channelized E1/ISDN PRI balanced networkmodule
NM-1CE1U	1-port channelized E1/ISDN PRI unbalancednetwork module
NM-2CE1B	2-port channelized E1/ISDN PRI balanced networkmodule
NM-2CE1U	2-port channelized E1/ISDN PRI unbalancednetwork module
NM-4B-S/T	4-port ISDN BRI network module
NM-4B-U	4-port ISDN BRI with NT1 networkmodule
NM-8B-S/T	8-port ISDN BRI network module (S/T interface)
NM-8B-U	8-port ISDN BRI with NT1 network module (U interface)
Modem Modules	
WIC-1AM	1-port analog modem WAN interface card (WIC)
WIC-2AM	2-port analog modem WAN interface card (WIC)
NM-6DM	6-port digital modem network module
NM-12DM	12-port digital modem networkmodule
NM-18DM	18-port digital modem networkmodule
NM-24DM	24-port digital modem networkmodule
NM-30DM	30-port digital modem networkmodule
NM-8AM	8-port analog modemNetwork Module
NM-16AM	16-port analog modemNetwork Module
NM-8AMJ	8-port analog modem NetworkModule—Japan
NM-16AMJ	16-port analog modemNetwork Module—Japan
Digital Subscriber Line (DSL)	
WIC-1ADSL	1-port ADSL WAN Interface Card
WIC-G.SHDSL	1-port G.shdsl WAN Interface Card
Encryption Advanced Integration Modules	
AIM-COMPR4	Data Compression AIM for3660 Series (4 E1 performance)
AIM-VPN/HP	DES/3DES VPN Encryption AIMfor 3660-High Performance
AIM-VPN/EPDES/3DES	VPN Encryption AIM for2600-Enhanced Performance
Content Engine Network Modules	
NM-CE-BP-20G-K9	Content EngineNetwork Module, Basic Performance, 20GB IDE Hard Disk
NM-CE-BP-40G-K9	Content EngineNetwork Module, Basic Performance, 40GB IDE Hard Disk
NM-CE-BP-SCSI-K9	Content EngineNetwork Module, Basic Performance, SCSI Controller
Dry Contact Closure Alarm NM	
NM-AIC-64	Alarm Monitoringand Control NetworkModule
Cisco EtherSwitch Modules	
NM-16ESW	One 16-Port 10/100 EtherSwitch Network Module
NM-16ESW-PWR	One 16 port 10/100 EtherSwitch NM with Inline Power support
NM-16ESW-1GIG	One 16 port 10/100 EtherSwitch NM with 1 GE (1000BaseT) port
NM-16ESW-PWR-1GIG	One 16 port 10/100 EtherSwitch NM withInline Powerand GE
PPWR-DCARD-16ESW	One Inlinepower daughter card for16 port EtherSwitch NM
NMD-36-ESW	One 36 port 10/100 EtherSwitch HighDensity Service Module
NMD-36-ESW-PWR	One 36 port 10/100 EtherSwitch HDSM withInline Power
NMD-36-ESW-2GIG	One 36 port 10/100 EtherSwitch HDSM withtwo GE (1000BaseT)
NMD-36-ESW-PWR-2G	One 36 port 10/100 EtherSwitch HDSM+ Inline Power and two GE
PPWR-DCARD-36ESW	One Inline Power daughter card for36 port EtherSwitch HDSM
GE-DCARD-ESW	One GE (1000BaseT) daughter cardfor EtherSwitch Modules
PPWR-PS-360W	One 48V (360W) power supply for EtherSwitch Modules
PPWR-PS-CHASSIS	One power supply chassis for Cisco 48V (360W) power supply
PWR-CHASSIS-360W	One power supply chassis and 48V power supply for EtherSwitch
CAB-PPWR-PS1-1	Connectsone EtherSwitch power supply to one EtherSwitch Module
CAB-PPWR-PS1-2	Connectsone EtherSwitch power supply to two EtherSwitch Modules
CAB-PPWR-PS2-1	Connectstwo EtherSwitch power supplies to one EtherSwitch Module

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the Distribution Product Reference Guide at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco 3600 Series Web site: **http://www.cisco.com/go/3700**

Cisco 7200 Series

The Cisco 7200 Series routers deliver exceptional price/performance, versatility, and feature-richness in a compact form factor. The Cisco 7200 is ideal as a WAN aggregator for the Service Provider (small POP) or enterprise edge, an enterprise WAN gateway, a high-end managed CPE, or as a small core router. The platform also supports sites that require IBM data center connectivity as well as sites that require multifunction capabilities that combine all the above for multiservice voice, video, and data traffic.

A key strength of the Cisco 7200 is its modularity. With a choice of 4- and 6-slot chassis, a selection of processors providing up to 1 Mpps, an extensive range of LAN and WAN interfaces with up to 48 ports per chassis, and single or dual power supplies, the customer can customize their system to achieve the performance, connectivity, and capacity desired. This modularity combined with a low initial price point guarantees both investment protection and maximum return on investment, allowing the customer to upgrade and/or redeploy their Cisco 7200 as their network needs change.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7204VXR	• 4-slot chassis • Modular processor: 225, 400, 900 Kpps (NPE-225, NPE-400, NPE-G1) or 300 Kpps service accelerator (NSE-1) • 1.2 Gbps backplane • MIX-enabled busfor data/voice/video applications
Cisco 7206VXR	• 6-slot chassis • Modular processor: 225, 400, 900 Kpps (NPE-225, NPE-400, NPE-G1) or 300 Kpps service accelerator (NSE-1) • 1.2 Gbps backplane • MIX-enabled busfor data/voice/video applications

Key Features

- Compact Form Factor—Up to six port adapters in a fully modular 3RU form factor. The optional Rack Density System (RDS) allows for up to nine Cisco 7206 routers per rack with front-to-back airflow
- Exceptional Value—As the most powerful single-processor platform, the Cisco 7200 offers customers a superior price/performance ratio supporting high-speed media and high-density configurations with up to 900 Kpps processing at a competitive price point
- Feature Rich—Full support for Cisco IOS software and enhancements for high-performance network services enables the Cisco 7200 to offer industry-leading network services, including: MPLS, broadband aggregation, quality of service (QoS), security, and voice/video/data support
- Connectivity/Flexibility—Provides high port density and an extensive range of LAN and WAN media, the Cisco 7200 dramatically reduces the cost per port and allows for flexible configurations to meet your specific network needs
- Common port adapters—Port adapters are shared with the Cisco 7300, 7400, 7500, and 7600 (w/FlexWAN Module), which simplifies sparing and protects customer investment in interfaces

Competitive Products

- Redback: SMS-500, SMS-1800
- Juniper: M5, M10
- Unisphere: ERX700, ERX1400

Specifications

Feature	Cisco 7204VXR	Cisco 7206VXR
Fixed Ports	None	Same as 7204VXR
Expansion Slots	4	6
WAN Port Adapters	DS0 to OC-12	Same as 7204VXR
Processor	RM7K RISC Processor with optional PXF Processor	Same as 7204VXR
Forwarding Rate	Up to 1 Mpps	Same as 7204VXR
Backplane Capacity	1.2 Gbps	Same as 7204VXR
Flash PCMCIA Memory	48 MB (expandable to 256 MB)	Same as 7204VXR
System DRAM Memory	128 MB (expandableto 1 GB)	Same as 7204VXR
Minimum Cisco IOS Release	12.0(1)XE	Same as 7204VXR
Internal Power Supply	AC or DC, dual option	Same as 7204VXR
Redundant Power Supply	Yes, for AC or DC	Same as 7204VXR
Chassis Height	3 RU	Same as 7204VXR
Rack Mountable	Yes, up to 16 per rack	Same as 7204VXR
Dimensions (HxWxD)	5.25 x 16.8 x 17 in.	Same as 7204VXR

Cisco IOS Software and Memory Requirements[1]

To run the Cisco IOS Feature Packs, you need, at a minimum, the amount of memory shown in the following table. Some configurations will require more.

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required	DRAM Memory Required
CD72-C-12.1T=	IP	12.1T	16MB	64MB
CD72-CK2-12.1E=	IP IPSEC 3DES	12.1E	16MB	64MB
CD72-CHK2-12.1T=	IP/FW/IDS IPSEC 3DES	12.1T	16MB	64MB
CD72-A-12.1T=	Enterprise	12.1T	16MB	64MB

1. For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information." For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

Selected Part Numbers and Ordering Information[1]

Cisco 7204 Chassis	
CISCO7204VXR	Cisco 7204VXR, 4-slot chassis, 1 AC Supply w/IP Software
CISCO7204VXR/225	7204VXR Bundle with NPE-225 and I/O Controller with 2 FE/E
Cisco 7206 Chassis	
CISCO7206VXR	Cisco 7206VXR, 6-slot chassis, 1 AC Supply w/IP Software
C7206VXR/400/2FE	7206VXR with NPE-400 and I/O Controller with 2 FE/E Ports
C7206VXR/400/GE	7206VXR with NPE-400 and GE+E I/O controller
7206VXR/NPE-G1	7206VXR with NPE-G1 processing engine
Cisco 7200 CPE Bundles	
7204VXR/CPE	7204VXR w/ NPE-225, 2 FE I/O, choice of specfied WAN PA
Cisco 7200 Voice Bundles	
C7206VXR/VOICE/400	7206VXR w/ NPE-400, Voice PA PA-VXC-2TE1+, I/O contlrw/ 2FE
Cisco 7200 VPN Bundle	
7204VXR/VPN/400K9	7204VXR VPN Bundle NPE400,128MB, I/O 2FE, ISA,IPSEC 3DES IOS
7204VXR400/VPNK9	7204VXR VPN Bundle NPE400,128MB, I/O 2FE, VAM,IPSEC 3DES IOS
7204VXR225/VPNK9	7204VXR VPN Bundle NPE225,128MB, I/O 2FE, VAM,IPSEC 3DES IOS
7206VXR400/VPNK9	7206VXR VPN Bundle NPE400,256MB, I/O 2FE, VAM,IPSEC 3DES IOS
7206VXRG1/VPNK9	7206VXR VPN Bundle NPE-G1,256MB, 3 FE/GE, VAM,IPSEC 3DES IOS

Cisco 7200 Series Processors

NPE-G1=	Cisco 7200 Network Processing Engine NPE-G1 including 256MB default DRAM and 64MB default flash memory.
NPE-225=	Network Processing Engine 225 (128MB default memory)-spare
NPE-400=	7200VXR NPE-400 (128MB default memory),SPARE
NSE-1=	7200VXR Network Services Engine 1 (128MB default mem),SPARE

Cisco 7200 Series Input/Output Controller

C7200-I/O=	Cisco 7200 Input/Output Controller, Spare
C7200-I/O-2FE/E=	Cisco 7200 Input/Output Controlle with Dual 10/100 Ethernet
C7200-I/O-GE+E=	Cisco 7200 Input/Output Controller with GE and Ethernet

Cisco 7200 Rack Mount Systems

CISCO7200RDS	CISCO 7200 Rack Density System

Cisco 7200 Processor Memory: NPE-G1

MEM-NPE-G1-256MB=	Two 128MB memory modules (256MB total) for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-512MB=	Two 256MB memory modules (512MB total) for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-1GB=	Two 512MB memory modules (1GB total) for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-FLD64=	64MB Compact Flash Disk for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-FLD128=	128MB Compact Flash Disk for the Cisco 7200 Network Processing Engine NPE-G1
MEM-NPE-G1-FLD256=	256MB Compact Flash Disk for the Cisco 7200 Network Processing Engine NPE-G1

Cisco 7200 Processor Memory: NPE-100, NPE-150, NPE-200

MEM-NPE-16MB=	16MB Memory Upgrade Kit for NPE-200/NPE-150/NPE-100
MEM-NPE-32MB=	32MB Memory Upgrade Kit for NPE-200/NPE-150/NPE-100
MEM-NPE-64MB=	2 32MB memory modules(64MB total) for NPE-200/NPE-150/NPE-100
MEM-NPE-128MB=	128MB Memory Upgrade Kit for NPE-200/NPE-150/NPE-100

Cisco 7200 Processor Memory: NPE-175 and NPE-300

MEM-SD-NPE-32MB=	32MB Memory Upgrade Kit for NPE-300/NPE-225/NPE-175
MEM-SD-NPE-64MB=	64MB Memory Upgrade Kit for NPE-300/225/175
MEM-SD-NPE-128MB=	128MB Memory Upgrade Kit for NPE-300/NPE-225/NPE-175
MEM-SD-NPE-256MB=	2 128MB memory modules (256MB total) for the NPE-300 in 7200

Cisco 7200 Processor Memory: NPE-225 and NSE-1

MEM-SD-NPE-128MB=	128MB Memory Upgrade Kit for NPE-300/NPE-225/NPE-175
MEM-SD-NSE-256MB=	256MB Memory for NPE-225 or NSE-1 in 7200 Series, SPARE

Cisco 7200 Processor Memory: NPE-400

MEM-NPE-400-128MB=	128MB Memory for NPE-400 in 7200 Series
MEM-NPE-400-256MB=	256MB Memory for NPE-400 in 7200 Series
MEM-NPE-400-512MB=	512MB Memory for NPE-400 in 7200 Series

Cisco 7200 Series Input/Output Controller Memory Options

MEM-CIP-32M=	CIP 32 MB DRAM Upgrade Kit
MEM-CPA-32M=	CPA 32MB DRAM Upgrade Kit
MEM-I/O-FLC20M=	Cisco 7200 I/O PCMCIA Flash Memory, 20MB
MEM-I/O-FLC8M=	Cisco 7200 I/O PCMCIA Flash Memory, 8MB
MEM-I/O-FLD128M=	Cisco 7200 I/O PCMCIA Flash Disk, 128 MB Spare
MEM-I/O-FLD48M=	Cisco 7200 I/O PCMCIA Flash Disk, 48 MB Spare

Cisco 7200 Series Port Adapters

PA-4C-E=	1 Port Enhanced ESCON Channel Port Adapter
PA-A2-4E1XC-E3ATM=	CES Port Adapter E3/E1 120 ohms
PA-A2-4E1XC-OC3SM=	CES OC3 Port Adapter4E1 Ports 120ohms
PA-A2-4T1C-OC3SM=	ATM CES Port Adapter, 4T1 CES Ports and 1 OC3 ATM SM Port
PA-A2-4T1C-T3ATM=	ATM CES Port Adapter, 4T1 CES Ports and 1 T3 ATM Port
PA-GE=	Gigabit Ethernet Port Adapter
PA-MCX-2TE1=	Spare 2 port MIX-enabled multichannel T1/E1 PA with CSU/DSU
PA-MCX-4TE1=	4 port MIX-enabled multichannelT1/E1 PA with CSU/DSU
PA-MCX-8TE1-M=	T1/E1 SS7 link PA for ITP
PA-MCX-8TE1=	8 port MIX-enabled multichannel T1/E1 with CSU/DSU
PA-SRP-OC12MM=	DPT-OC12 Multi-mode port adapter
PA-SRP-OC12SMI=	DPT-OC12 Single-mode intermediate port adapter
PA-SRP-OC12SML=	DPT-OC12 Single-mode long-reachport adapter
PA-SRP-OC12SMX=	DPT-OC12 Singe-mode extended reach PA

Cisco 7200, 7400 and 7500 Series Port Adapters

PA-VXC-2TE1+=	2 port TE1 hi-capacity enhanced voice PA
PA-VXB-2TE1+=	2 port T1/E1 moderate capacity enhanced voice PA
PA-T3=	1 Port T3 Serial Port Adapterwith T3 DSUs
PA-T3+=	1 Port T3 Serial Port Adapter Enhanced
PA-POS-OC3SML=	1-Port Packet/SONET OC3c/STM1 Singlemode (LR) PA
PA-POS-OC3SMI=	1-Port Packet/SONET OC3c/STM1 Singlemode (IR)PA
PA-POS-OC3MM=	1-Port Packet/SONET OC3c/STM1 Multimode PA
PA-POS-2OC3=	2 Port Packet/SONET OC3c/STM1 Port Adapter
PA-MC-T3=	1 port multichannel T3port adapter
PA-MC-E3=	1 port Multi-Channel E3port adapter
PA-MC-4T1=	4 port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-2T3+=	2 port multichannel T3port adapter
PA-MC-2T1=	2 port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-2E1/120=	2 port multichannel E1 port adapter with G.703 120ohm interf
PA-H=	Port Adapter: 1-Port HSSI
PA-E3=	1 Port E3 Serial Port Adapterwith E3 DSU
PA-A3-T3=	1-Port ATM Enhanced DS3Port Adapter (Spare)
PA-A3-OC3SML=	1-Port ATM Enhanced OC3c/STM1 Singlemode(LR)Port Adapter
PA-A3-OC3SMI=	1-Port ATM Enhanced OC3c/STM1 Singlemode(IR)Port Adapter
PA-A3-OC3MM=	1-Port ATM Enhanced OC3c/STM1 Multimode Port Adapter
PA-A3-E3=	1-Port ATM Enhanced E3 Port Adapter (Spare)
PA-A3-8E1IMA=	8-port ATM Inverse Mux E1 (120 Ohm) Port Adapter, Spare
PA-8T-X21=	8-Port Serial, X.21 Port Adapter
PA-8T-V35=	8-Port Serial, V.35 Port Adapter
PA-8T-232=	8-Port Serial, 232 Port Adapter
PA-8E=	8-Port Ethernet 10BaseT Port Adapter
PA-4T+=	4-Port Serial Port Adapter, Enhanced
PA-4E1G/75=	4-Port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
PA-4E1G/120=	4-Port E1 G.703 Serial Port Adapter (120ohm/Balanced)
PA-4E=	4-Port Ethernet 10BaseT Port Adapter
PA-2T3=	2 Port T3 Serial Port Adapterwith T3 DSUs
PA-2T3+=	2 Port T3 Serial Port Adapter Enhanced,Spare
PA-2H=	PORT ADAPTER:2-PORT HSSI
PA-2FE-TX=	2-Port Fast Ethernet 100Base TX Port Adapter
PA-2FE-FX=	2-Port Fast Ethernet 100Base FX Port Adapter
PA-2E3=	2 Port E3 Serial Port Adapterwith E3 DSUs

Cisco 7200 and 7400 Series Port Adapters

PA-8B-S/T=	8-Port BRI Port Adapter, S/T Interface

Cisco 7200 and 7500 Series Port Adapters

PA-VXA-1TE1-30+=	1 Port T1/E1 Digital Voice Port Adapterwith 30 Channels
PA-VXA-1TE1-24+=	1 Port T1/E1 Digital Voice Port Adapterwith 24 Channels
PA-MC-STM-1SMI=	1 port multichannel STM-1 single mode port adapter
PA-MC-STM-1MM=	1 port multichannel STM-1multimode port adapter
PA-MC-8TE1+=	8 port multichannel T1/E1 8PRI port adapter
PA-F/FD-SM=	1-Port FDDI Full Duplex Single-Mode Port Adapter
PA-F/FD-MM=	1-Port FDDI Full Duplex Multi-Mode Port Adapter
PA-A3-8T1IMA=	8-port ATM Inverse Mux T1 Port Adapter, Spare
PA-4R-DTR=	Port Adapter:4-Port Dedicated Token Ring,4/16Mbps, HDX/FDX

Cisco 7200 Series Service Adapters

SA-ISA=	Integrated Services Adapter for IPSec or MPPE encryption
SA-VAM=	VPN Acceleration Module (VAM)IPSec and IPComp Acceleration

Cisco 7200 Series Transceiver Modules

GBIC-LX/LH=	Gigabit Interface Converterfor 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. Converter For 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX
POM-OC3-MM	1-port OC3/STM1 Pluggable Optic Module,MM
POM-OC3-SMIR	1-port OC3/STM1 Pluggable Optic Module, SM-IR
POM-OC3-SMLR	1-port OC3/STM1 Pluggable Optic Module, SM-LR

Cisco 7200 Series Power Supplies	
PWR-7200-DC+=	Cisco 7200 DC (24V-60V) Power Supply Option
PWR-7200/2-DC+	Cisco 7200 Dual DC (24V-60V) Power Supply Option
PWR-7200-AC=	Cisco 7200 AC Power Supply With United States Cord
PWR-7200-ACA=	Cisco 7200 AC Power Supply With Australian Cord
PWR-7200-ACE=	Cisco 7200 AC Power Supply With European Cord
PWR-7200-ACI=	Cisco 7200 AC Power Supply With Italian Cord
PWR-7200-ACU=	Cisco 7200 AC Power Supply With United Kingdom Cord
Cisco 7200 Series Spares and Accessories	
ACS-7200-RMK=	Cisco 7200 Rackmount Kit and Cable Management Bracket
CVPN7200FIPS/KIT=	Kit(Instructions,labels)to configure 7206 for FIPS operation

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 7200 Series Web site: **http://www.cisco.com/go/7200**

Cisco 7300 Series

The Cisco 7300 Series Routers are optimized for flexible, high performance IP/MPLS services at the network edge, where service providers and enterprises link together. Coupled with powerful network processing, a broad set of interfaces and a compact, modular form factor the Cisco 7300 Series Routers are ideal for intelligent, multi-gigabit network connectivity.

The Cisco 7304 Series Router is ideally applied as a high-end CPE or as an Internet Gateway router. Architected for network High Availability and multi-protocol support, the 7304 supports the broad set of existing Cisco 7000 Series Port Adapters with the new Cisco 7304 Port Adapter Carrier Card.

The Cisco 7301 Series Router is a compact single rack unit router coupled with a broad set of interfaces and Cisco IOS software features. It packs high performance in a space and power efficient form factor that includes a single 7000 Series port adapter slot, 3 on-board Gigabit Ethernet (copper or optical)/Fast Ethernet ports and a new high-speed bus technologies.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7301	• Compact, power efficient 1RU form factor • Three times the performance increase over existing single rack unit routers like the Ciso 7401 • Single 7000 Series Port Adapter Slot
Cisco 7304	• Highly modular price and performance optmized platform, rich in IP services • High performance connectivity—DS-1 through OC48/STM16 with 3.5 Mpps performance • Built-in Gigabit Ethernet connectivity • Multiprotocol routing:IP, IPX, AppleTalk, DLSw • Compact size, high availability and optimal cooling

Key Features

- Cisco 7301: With nearly 1 million-packets-per-second (Mpps) processing performance, the fastest Cisco 1RU general-purpose processor, as of January 2003; 3 fixed 10/100/1000-Mbps ports (RJ-45 or SFP optics) directly on the processor; Full Cisco IOS feature support; Pluggable Gigabit Ethernet optics (SFPs); Up to 1GB of available DRAM; Up to 256MB of removable compact flash memory; Front-back airflow and single sided management
- Cisco 7304: Compact modular form factor with four RU with four port adapter slots per chassis; PXF IP processor hardware-accelerated services such as Cisco Express Forwarding (CEF), NetFlow v8, and Turbo ACL; Offers 3.5Mpps performance for PXF-accelerated services with the NSE-100 Network Services Forwarding Engine; Two Gigabit Ethernet ports per NSE-100; System redundancy: optional dual processors and dual AC or DC power supplies increases network availability

Competitive Products

- Redback: SMS-500, SMS-1800
- Juniper: M5, M10
- Unisphere: ERX700, ERX1400

Specifications

Feature	Cisco 7301	Cisco 7304
Fixed Ports	Three Gigabit Ethernet ports	Same as 7301
Expansion Slots	1	4
WAN Interface Range	DS-1 to OC-3	T3 to OC-48
Processor	RM 7000 MIPS Processor + PXF Processor	RM 7000 MIPS Processor + PXF Processor
Forwarding Rate	Up to 1 Mpps	Up to 3.5 Mpps
Backplane Capacity	1.2 Gbps	16 Gbps
Flash PCMCIA Memory	64 MB (expandable to 128 MB)	Same as 7301
System DRAM Memory	128 MB (expandableto 512 MB)	Same as 7301
Minimum Cisco IOS Release	12.2(11)YZ	12.1(9)EX
Internal Power Supply	AC or DC	Same as 7301
Redundant Power Supply Support	Yes, for AC or DC	Same as 7301
Chassis Height	1 RU	4 RU
Rack Mountable	Yes, up to 40 per rack	Yes, up to 11 per rack
Dimensions (HxWxD)	1.73 x 17.3 x 13.87 in.	7 x 17.2 x 20.5 in.

Selected Part Numbers and Ordering Information[1]

Cisco 7300 System

PWR-7301-AC	Cisco 7301 AC Power Supply Option
PWR-7301/2-AC	Cisco 7301 Dual AC Power Supply Option
PWR-7301-DC48	Cisco 7301 DC48 Power Supply Option
PWR-7301/2-DC48	Cisco 7301 Dual DC48 Power Supply Option
PWR-7301-DC24	Cisco 7301 DC24 Power Supply Option
CISCO7301	Cisco 7301 chassis, 256MB memory, A/C power,64MB Flash
CISCO7304=	Cisco 7300, 4-slot chassis
CISCO7304-CH	Cisco7304 channel bundle
7300-NSE-100=	Cisco 7304 Network Services Engine 100
7300-NSE-100/2	Redundant Cisco 7304 NSE-100 w/Redundancy Feature License
7300-PWR-DC=	Cisco 7304 DC Power Supply Spare
7300-PWR-AC=	Cisco 7304 AC Power Supply Spare
7300-PWR/2-DC	Cisco 7304 Redundant DC Power Supply Option
7300-PWR/2-AC	Cisco 7304 Redundant AC Power Supply Option

Cisco 7300 Memory Options

MEM-7301-1GB=	1GB memory upgrade for 7301
MEM-7301-512MB=	512MB memory upgrade for 7301
MEM-7301-256MB=	256MB memory upgrade for Cisco 7301
7300-MEM-128=	128MB default SDRAM for 7304 NSE-100, spare
7300-MEM-256=	256MB SDRAM for 7304 NSE-100, spare
7300-MEM-512=	512MB SDRAM for 7304 NSE-100, spare
7300-I/O-CFM-64M=	Cisco 7304 Compact Flash Memory, 64 MB
7300-I/O-CFM-128M=	Cisco 7304 Compact Flash Memory, 128 MB

Cisco 7300 Series Compact Flash Disk Options

MEM-7301-FLD64=	Compact Disk Flash for 7301,64MB option
MEM-7301-FLD128=	Compact Disk Flash for 7301, 128MB option
MEM-7301-FLD256	Compact Disk Flash for 7301, 256MB Option

Cisco 7300 Line Cards

7300-1OC12POS-MM=	1-port OC12 POS line card for Cisco7304 w/ Multi-mode
7300-1OC12POS-SMI=	1-port OC12 POS line card for Cisco 7304 w/ Single-mode IR
7300-1OC12POS-SML=	1-port OC12 POS line card for Cisco 7304 w/ Single-mode LR
7300-1OC48POS-SMI=	1-port OC48 POS line card for Cisco 7304 w/ Single-mode IR
7300-1OC48POS-SML=	1-port OC48 POS line card for Cisco 7304 w/ Single-mode LR
7300-1OC48POS-SMS=	1-port OC48 POS line card for Cisco 7304 w/ Single-mode SR
7300-2OC12POS-MM=	2-port OC12 POS line card for Cisco7304 w/ Multi-mode
7300-2OC12POS-SMI=	2-port OC12 POS line card for Cisco 7304 w/ Single-mode IR
7300-2OC12POS-SML=	2-port OC12 POS line card for Cisco 7304 w/ Single-mode LR
7300-2OC3ATM-MM=	2-port OC3 ATM line card for Cisco 7304 w/ Multi-mode
7300-2OC3ATM-SMI=	2-port OC3 ATM line card for Cisco 7304 w/ Single-mode IR
7300-2OC3ATM-SML=	2-port OC3 ATM line card for Cisco 7304 w/ Single-mode LR
7300-2OC3POS-MM=	2-port OC3 POS line card for Cisco 7304 w/ Multi-mode
7300-2OC3POS-SMI=	2-port OC3 POS line card for Cisco 7304 w/ Single-mode IR
7300-2OC3POS-SML=	2-port OC3 POS line card for Cisco 7304 w/ Single-mode LR
7300-4OC3POS-MM=	4-port OC3 POS line card for Cisco 7304 w/ Multi-mode
7300-4OC3POS-SMI=	4-port OC3 POS line card for Cisco 7304 w/ Single-mode IR
7300-4OC3POS-SML=	4-port OC3 POS line card for Cisco 7304 w/ Single-mode LR
7300-6T3=	6-port T3 line card for Cisco 7304 w/ DSU

Cisco 7300 Series Transceiver Modules

GBIC-LX/LH=	Gigabit Interface Converter for 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. ConverterFor 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX

Cisco 7300 Accessories

7300-HALFSLOTBLNK	Cisco 7304 Half Slot Blank Line Card
7300-4RU/RCKBRKT=	Cisco 7304 Chassis Rackmount Bracket Spare
7300-CNTR-SPTUM=	Cisco 7304 Center Septum Spare

Cisco 7300 Software Options

S73A-12215B=	Cisco 7301 Series IOS ENTERPRISE
S73AH-12215B=	Cisco 7301 Series IOS ENTERPRISE/FW/IDS
S73AHK8-12215B=	Cisco 7301 Series IOS ENTERPRISE/FW/IDS IPSEC 56
S73AHK9-12215B=	Cisco 7301 Series IOS ENTERPRISE/FW/IDS IPSEC 3DES
S73AS-12215B=	Cisco 7301 Series IOS ENTERPRISE SSG
S73C-12215B=	Cisco 7301 Series IOS IP
S73A-12211YZ=	Cisco 7300 Series IOS ENTERPRISE
S73C-12211YZ=	Cisco 7300 Series IOS IP PLUS
S730A-12211YZ=	Cisco 7301 Series IOS ENTERPRISE
S730C-12211YZ=	Cisco 7301 Series IOS IP
S730Z-12211YZ=	Cisco 7301 Series IOS SERVICE PROVIDER
S73A-12113EX=	Cisco 7300 IOS ENTERPRISE
S73AHK2-12113EX=	Cisco 7300 IOS ENTERPRISE/FW/IDS IPSEC 3DES
S73AHL-12113EX=	Cisco 7300 IOS ENTERPRISE/FW/IDS IPSEC 56
S73AR1P-12113EX=	Cisco 7300 IOS CISCO 7300 SERIES IOS ENTERPRISE/SNASW PLUS
S73CHK2-12113EX=	Cisco 7300 IOS IP/FW/IDS IPSEC 3DES
S73CHL-12113EX=	Cisco 7300 IOS IP/FW/IDS IPSEC 56
S73CP-12113EX=	Cisco 7300 IOS IP PLUS
S73A-12112EX=	Cisco 7300 IOS ENTERPRISE
S73AHK2-12112EX=	Cisco 7300 IOS ENTERPRISE/FW/IDS IPSEC 3DES
S73AHL-12112EX=	Cisco 7300 IOS ENTERPRISE/FW/IDS IPSEC 56
S73AR1P-12112EX=	Cisco 7300 IOS CISCO 7300 SERIES IOS ENTERPRISE/SNASW PLUS
S73CHK2-12112EX=	Cisco 7300 IOS IP/FW/IDS IPSEC 3DES
S73CHL-12112EX=	Cisco 7300 IOS IP/FW/IDS IPSEC 56
S73CP-12112EX=	Cisco 7300 IOS IP PLUS

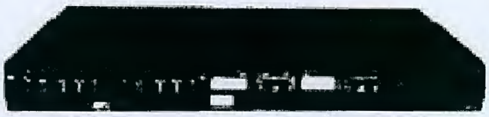
Cisco 7300 Carrier Cards	
7300-CC-PA=	7304 Carrier Card for 7200 Series Port Adapters
SFPs for Cisco 7301 Series	
GLC-SX-MM=	GE SFP, LC connector SXtransceiver
GLC-LH-SM=	GE SFP, LC connector LHtransceiver

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 7300 Series Web site: **http://www.cisco.com/go/7300**

Cisco 7400 Series



With the Cisco 7400, this modular, one-port adapter slot unit leverages over 40 standard 7200/7500 series port adapters. Its compact, stackable architecture is designed for application specific routing deployments, such as broadband services aggregation (PPP/L2TP) and WAN edge connectivity in service provider and enterprise networks. Leveraging Cisco patented technology, the Cisco 7400 series delivers a premium suite of hardware-accelerated network services.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7401ASR-CP	• General WAN edge connectivity in a small form factor, or as managed customer premise equipment (CPE) • Broad range of connectivity options—from DS0 to OC-3 interfaces • Comprehensive management services with remote management, provisioning, trouble shooting and software upgrade • Hardware accelerated services, including: NAT, ACLs, Netflow, CBWFQ, CBWRED, Policing, marking, Hierarchical Traffic Shaping, & VRF lite
Cisco 7401ASR-BB	• Complete broadbandsubscriber services suite with highest subscribers per rack ratio • One fast LAN interface (FE/GE) and one fast WAN interface (DS3/OC3) • High volume/densityof PPP, PPPoE, PPPoA, L2TP tunnel aggregation and termination for broadband services like DSL, Cable, and Wireless

Key Features

- Compact form factor with 1 RU, front-to-back airflow and stackability
- Hardware—accelerated IP network services
- Built-in dual GE connectivity
- Flexible WAN connectivity supporting over 40 interfaces including serial, multichannel, ISDN, Frame Relay, ATM, Packet over SONET (POS), from NxDS0 to OC-3
- Shared port adaptors with the Cisco 7200, 7300, 7500, and 7600 (with FlexWAN Module), which simplifies sparing and protects customer investment in interfaces

Competitive Products

- Redback: SMS500, SMS1800
- Juniper: M5, M10
- Unisphere: ERX700, ERX1400

Specifications

Feature	Cisco 7401ASR-BB	Cisco 7401ASR-CP
Fixed Ports	2 Gigabit Ethernet (RJ or GBIC) ports	Same as 7401ASR-BB
Expansion Slots	1	Same as 7401ASR-BB
WAN Interface Range	DS0 to OC-3	Same as 7401ASR-BB
Processor	RM7K RISC Processor + PXF Processor	Same as 7401ASR-BB
Forwarding Rate	Up to 350 Kpps	Same as 7401ASR-BB
Backplane Capacity	1.2 Gbps	Same as 7401ASR-BB
Flash PCMCIA Memory	64MB (expandable to 128MB)	Same as 7401ASR-BB
System DRAM Memory	256MB (expandable to512MB)	128MB (expandable to 512MB)
Minimum Cisco IOS Release	12.2(1)DX	Same as 7401ASR-BB
Internal Power Supply	AC, DC48V, DC24V, or Dual DC48V	Same as 7401ASR-BB
Redundant Power Supply Support	Yes	Same as 7401ASR-BB
Chassis Height	1 RU	Same as 7401ASR-BB
Rack Mountable	Yes, up to 40 per rack	Same as 7401ASR-BB
Dimensions (HxWxD)	1.72 x 17.3 x 11.80 in	Same as 7401ASR-BB

Selected Part Numbers and Ordering Information[1]

Cisco 7400 ASR Bundles	
CISCO7401ASR-BB	7401ASR, 256M SDRAM, Broadband Featue License
CISCO7401ASR-CP	7401ASR,128M SDRAM, IP Software
CISCO7401-2DC48=	Cisco 7400 chassis with dual DC power supply
7401ASR-CPT3	7401ASR,256M SDRAM, PA-T3+
C7400VPN/K9	7400 VPNRouter w/VAM,VPN DeviceMgr, 2xFE/GE,AC PS,IPSEC 3DES
Cisco 7400 ASR Memory Options	
MEM-COMP-FLD64M=	Cisco 7400ASR Compact Flash Disk, 64 MB (spare)
MEM-COMP-FLD128M=	Cisco 7400ASR Compact Flash Disk, 128 MB (spare)
MEM-7400ASR-256MB=	256MB Spare memory for Cisco 7400ASR/VPN
MEM-7400ASR-512MB=	512MB Spare SDRAM for Cisco 7400ASR/VPN
Cisco 7400 ASR Transceiver Modules	
GBIC-LX/LH=	Gigabit Interface Converterfor 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. ConverterFor 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX
POM-OC3-MM	1-port OC3/STM1 Pluggable Optic Module,MM
POM-OC3-SMIR	1-port OC3/STM1 Pluggable Optic Module, SM-IR
POM-OC3-SMLR	1-port OC3/STM1 Pluggable Optic Module, SM-LR
Cisco 7400 and 7500 Series Port Adapters	
PA-POS-OC3MM=	1-Port Packet/SONET OC3c/STM1 Multimode PA
PA-MC-8E1/120=	8 port multichannel E1 port adapter with G.703 120ohm interf
PA-2FE-FX=	2-Port Fast Ethernet 100Base FX Port Adapter
Cisco7200, 7400 and 7500 Series Port Adapters[2]	
Cisco 7400 ASR Power Supplies and Cords	
CAB-AC=	AC Power Cord, US
CAB-ACA=	AC Power Cord, Australia
CAB-ACE=	AC Power Cord, Europe
CAB-ACI=	AC Power Cord, Italy
CAB-ACR=	Power Cord Argentina, Spare
CAB-ACU=	AC Power Cord, UK
Cisco 7400 Software Options	
S74CHK9-12209YE=	Cisco 7400 Series IOS IP/FW/IDS IPSEC 3DES
S74CK9-12209YE=	Cisco 7400 Series IOS IP PLUS IPSEC 3DES
S74A-12204B=	Cisco 7400 Series IOS ENTERPRISE
S74AH-12204B=	Cisco 7400 Series IOS ENTERPRISE/FW/IDS
S74AHK9-12204B=	Cisco 7400 Series IOS ENTERPRISE/FW/IDS IPSEC 3DES
S74AS-12204B=	Cisco 7400 Series IOS ENTERPRISE SSG
S74C-12204B=	Cisco 7400 Series IOS IP
S74A-12202DD=	Cisco 7400 Series IOS ENTERPRISE
S74AH-12202DD=	Cisco 7400 Series IOS ENTERPRISE/FW/IDS

Cisco 7400 VPN Memory Options	
MEM-COMP-FLD64M=	Cisco 7400ASR Compact Flash Disk, 64 MB (spare)
MEM-COMP-FLD128M=	Cisco 7400ASR Compact Flash Disk, 128 MB (spare)
MEM-7400ASR-256MB=	256MB Spare memory for Cisco 7400ASR/VPN
MEM-7400ASR-512MB=	512MB Spare SDRAM for Cisco 7400ASR/VPN
Cisco 7400 VPN Transceiver Modules	
GBIC-LX/LH=	Gigabit Interface Converterfor 1000BASE-LX standard
GBIC-SX=	Gigabit Intf. Converter for 1000BASE-SX (Short Wavelength)
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX
Cisco 7400 VPN Power Supplies and Cords	
CAB-AC=	AC Power Cord, US
CAB-ACA=	AC Power Cord, Australia
CAB-ACE=	AC Power Cord, Europe
CAB-ACI=	AC Power Cord, Italy
CAB-ACR=	Power Cord Argentina,Spare
CAB-ACU=	AC Power Cord, UK

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.
2. Cisco 7200, 7400 and 7500 share many port adapters. Please see Cisco 7200, 7400 and 7500 Series Port Adapters, page 1-34 for additional part numbers.

For More Information

See the Cisco 7400 Series Web site: **http://www.cisco.com/go/7400**

Cisco 7500 Series

An essential part of both Enterprise and Service Provider networks, the Cisco 7500 Series routers are the market leader for edge applications, due to its breadth of services, diverse interfaces, reliability, and performance. Since its inception, the Cisco 7500 has seen huge improvements in performance and its ability to scale, most recently with the Route Switch Processor 16 (RSP16) and Versatile Interface Processor 6-80 (VIP6-80) module. This series combines Cisco's proven software technology with exceptional reliability, availability, serviceability, and performance features to meet the requirements of today's most mission-critical networks.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7505	• 5 expansion slots • One CyBus • DS0 to OC-12 connectivity (all platforms)
Cisco 7507	• 7 expansion slots • Dual CyBuses • Redundant powersupplies • Diverse set of routingprotocols (allplatforms)
Cisco 7513	• 13 expansion slots • Dual CyBuses • Redundant powersupplies • Diverse set of routingprotocols (allplatforms)

Key Features

- High-performance switching—Delivers high performance for mission-critical applications by supporting high-speed media and high-density configurations; using the processing capabilities of the Versatile Interface Processors and Cisco Express Forwarding—the Cisco 7500 series system capacity can exceed two million packets per second
- Full support for Cisco IOS software and enhancements for high-performance network services—Performs network services such as quality of service, security, compression, and encryption at high speed; VIP technology extends the performance of these services through distributed IP services
- High port density—Provides high port density and an extensive range of LAN and WAN media; this feature dramatically reduces the cost per port and allows a flexible configuration
- Unmatched interface flexibility—The Cisco 7500 supports a broad selection of Interface Processors (IPs) and Port Adapters (PAs). Port adapters are shared with the Cisco 7200, 7400, and 7600 (with FlexWAN Module)
- High Availability—Enhanced features and capabilities include redundant route processors, power supplies, fans, and software fault isolation with Stateful Switchover and NonStop Forwarding

Competitive Products

• Redback: SMS-500, SMS-1800	• Unisphere: ERX700, ERX1400
• Juniper: M5, M10, M20	• Huawei: NE8 and NE16

Specifications

Feature	Cisco 7505	Cisco 7507	Cisco 7513
Fixed Ports	None	Same as Cisco 7505	Same as Cisco 7505
Expansion Slots	5	7	13
WAN Interface Range	DS0 to OC-12	Same as Cisco 7505	Same as Cisco 7505
Processor	MIPS RISC Processor	Same as Cisco 7505	Same as Cisco 7505
Forwarding Rate	Up to 1.1 Mpps	Up to 2.2 Mpps	Up to 2.2 Mpps
Backplane Capacity	1 Gbps	2 Gbps	2 Gbps
Flash PCMCIA Memory	16MB (expandable to128MB)	Same as Cisco 7505	Same as Cisco 7505
System DRAM Memory	32MB (expandable to1GB)	Same as Cisco 7505	Same as Cisco 7505
Minimum Cisco IOS Release	11.3	Same as Cisco 7505	Same as Cisco 7505
Internal Power Supply	AC or DC	AC, dual AC/DC, or dual DC	AC, dual AC/DC, or dual DC
Redundant Power Supply Support	No	Yes	Yes
Chassis Size	6 RU	13 RU	20 RU
Rack Mountable	Yes, up to 6 per rack	Yes, up to 3 per rack	Yes, up to 2 per rack
Dimensions (HxWxD)	10.5 x 17.5 x 17 in.	19.25 x 17.5 x 25 in.	33.75 x 17.5 x 22 in.

Selected Part Numbers and Ordering Information[1]

Cisco 7500 Series Products	
CISCO7505/4	Cisco 7505 5-Slot, 1 CyBus, 1RSP4, Single Power Supply
CISCO7507/8-MX	Cisco 7507, 7 Slot, MIX-Enabled, Dual Bus, 1 RSP8, 1 PS
CISCO7507/8X2-MX	Cisco 7507, 7 Slot, MIX-Enabled, Dual Bus, 2 RSP8, 2 PS
CISCO7507/4	Cisco 7507 7-Slot, 2 CyBus, 1RSP4, Single Power Supply
CISCO7507/4X2	Cisco 7507 7-Slot, 2 CyBus, 2 RSP4, Dual Power Supply
CISCO7513/4	Cisco 7513 13-Slot, Dual Bus, 1RSP4, 1 PS
CISCO7513/4X2	Cisco 7513 13-Slot, Dual Bus, 2 RSP4, 2 PS
CISCO7513/8-MX	Cisco 7513, 13 Slot, MIX-Enabled, Dual Bus, 1 RSP8, 1 PS
CISCO7513/8X2-MX	Cisco 7513, 13 Slot, MIX-Enabled, Dual Bus, 2 RSP8, 2 PS
CISCO7507/16-MX	Cisco 7507, 7 Slot, MIX-Enabled, Dual Bus, 1 RSP16, 1 PS
CISCO7507/16X2-MX	Cisco 7507, 7 Slot, MIX-Enabled, Dual Bus, 2 RSP16, 2 PS
CISCO7513/16-MX	Cisco 7513, 13 Slot, MIX-Enabled, Dual Bus, 1 RSP16, 1 PS
CISCO7513/16X2-MX	Cisco 7513, 13 Slot, MIX-Enabled, Dual Bus, 2 RSP16, 2 PS
Cisco 7500 Series Processors and Accessories	
RSP2=	CISCO 7507/7513 ROUTE SWITCH PROCESSOR SPARE
RSP2/2	DUAL RSP2 OPTION FOR 7507 and 7513
CAB-RSP2CON=	RSP2 Console Cable (Spare)
CAB-RSP2AUX=	RSP2 Auxiliary Cable (Spare)
RSP4+=	Cisco 7500 Series Route Switch Processor 4+ (Spare)
RSP8=	Cisco 7505/7507/7513/7576 Route Switch Processor (Spare)
RSP16=	CISCO 7500 ROUTE SWITCH PROCESSOR 16 Spare
Route Switch Processor Memory Options (RSP1 & RSP2)	
MEM-RSP-FLC8M=	RSP Flash Credit Card: 8 MB Kit
MEM-RSP-FLC16M=	RSP Flash Credit Card: 16 MB Kit
MEM-RSP-FLC20M=	RSP Flash Credit Card: 20 MB Kit
MEM-RSP-FLC32M=	RSP2 Flash Card: 32MB Kit
MEM-RSP-16M=	RSP 16 MB DRAM Upgrade Kit
MEM-RSP-32M=	RSP 32MB DRAM Upgrade Kit
MEM-RSP-64M=	RSP 64MB DRAM Upgrade Kit
MEM-RSP-128M=	RSP 128MB DRAM Upgrade Kit
Route Switch Processor Memory Options (RSP4)	
MEM-RSP4-FLC16M=	RSP4 Flash Card: 16 MB Kit
MEM-RSP4-FLC20M=	RSP4 Flash Card: 20 MB Kit
MEM-RSP4-FLC32M=	RSP4/4+ Flash Card: 32 MB Kit
MEM-RSP4-32M=	RSP4 32MB DRAM Upgrade Kit
MEM-RSP4-64M=	RSP4/RSP4+ 64MB DRAM Upgrade Kit
MEM-RSP4-128M=	RSP4/RSP4+ 128MB DRAM Upgrade Kit
MEM-RSP4-128-4PK=	RSP4 128MB DRAM Upgrade Kit (4-pack)
MEM-RSP4-256M=	RSP4/RSP4+ 256MB DRAM Upgrade Kit
MEM-RSP4-256-4PK=	RSP4 256MB DRAM Upgrade Kit (4-pack)
MEM-16F-RSP4+=	RSP4+ 16MB Boot Flash (Spare)
MEM-V250-128-10PK=	128 MByte DRAM Upgrade for VIP2-50/xIP-50 (10-pack)
Route Switch Processor Memory Options (RSP8)	
MEM-RSP8-64M=	RSP8 64MB DRAM Option
MEM-RSP8-128M=	RSP8 128MB DRAM Upgrade Kit
MEM-RSP8-256M=	RSP8 256MB DRAM Upgrade Kit
MEM-RSP8-FLC16M=	RSP8 Flash Card: 16 MB Kit
MEM-RSP8-FLC20M=	RSP8 Flash Card: 20 MB Kit
MEM-RSP8-FLC32M=	RSP8 Flash Card: 32 MB Kit
MEM-RSP8-FLD48M=	RSP8 Flash Disk: 48 MB Kit
MEM-RSP8-FLD128M=	RSP8 Flash Disk: 128 MB Kit
Route Switch Processor Memory Options (RSP16)	
MEM-RSP16-FLD48M=	RSP16 Flash Disk: 48 MB Option
MEM-RSP16-FLD128M=	RSP16 Flash Disk: 128 MB Option
MEM-RSP16-128M=	RSP16 128MB ECC SDRAM Memory Spare
MEM-RSP16-256M=	RSP16 256MB ECC SDRAM Memory Spare
MEM-RSP16-512M=	RSP16 512MB ECC SDRAM Memory Spare
MEM-RSP16-1G=	RSP16 1GB ECC SDRAM Memory Spare
CISCO7500 Series Gigabit Ethernet Interface Processor	
GEIP=	Gigabit Ethernet Interface Processor
GEIP+=	Enhanced Gigabit Ethernet

Cisco 7500 Series Interface Processors

CX-CIP2-ECA1=	CHANNEL IP:CIP2 W/ ECA-1 PORT
CX-CIP2-ECA2=	CHANNEL IP:CIP2 W/ ECA-2 PORTS
FEIP2-DSW-2TX=	2-Port Fast EthernetIP with Dist. Switching (100TX)
FEIP2-DSW-2FX=	2-Port Fast Ethernet IP with Dist. Switching (100FX)
CX-ECA1-U	ESCON Interface Upgrade for CX-CIP-ECA1 or CX-CIP-PCA1

Cisco 7500 Series Versatile Interface Processors

VIP2-40=	VERSATILE INT. PROCESSOR-2,MODEL 40
VIP2-50=	Versatile Interface Processor 2, Model 50
VIP2-10/15-UPG	VIP2-10 to VIP2-15 Upgrade
VIP2-10/40-UPG	VIP2-10 TO VIP2-40 UPGRADE
VIP2-15/40-UPG	VIP2-15 to VIP2-40 Upgrade
VIP2-20/40-UPG	VIP2-20 TO VIP2-40 UPGRADE
VIP4-50=	Versatile Interface Processor 4, Model 50
VIP4-80=	Versatile Interface Processor 4, Model 80
VIP6-80=	Services Accelerator Versatile Interface Processor 6-80

Cisco 7500 Series Transceiver Modules

GBIC-SX=	Gigabit Intf. ConverterFor 1000BASE-SX (Short Wavelength)
GBIC-LX/LH=	Gigabit Interface Converterfor 1000BASE-LX standard
GBIC-ZX=	Gigabit Interface Converterfor 1000 BASE-ZX
POM-OC3-MM	1-port OC3/STM1 Pluggable Optic Module,MM
POM-OC3-SMIR	1-port OC3/STM1 Pluggable Optic Module, SM-IR
POM-OC3-SMLR	1-port OC3/STM1 Pluggable Optic Module, SM-LR

Cisco 7500 VIP2 Memory Options

MEM-VIP240-32M	32 MB DRAM Option for VIP2-40 (Default)
MEM-VIP240-64M=	64 MB DRAM Option for VIP2-40 (Spare)
MEM-V240-64-10PK=	64 MByte DRAM Upgrade for VIP2-40 (10-pack)
MEM-V250-128-10PK=	128 MByte DRAM Upgrade for VIP2-50/xIP-50 (10-pack)
MEM-VIP250-32M-D=	32 Mbytes DRAM Option for VIP2-50/xIP-50 (default)
MEM-VIP250-64M-D=	64 Mbytes DRAM Option for VIP2-50/xIP-50
MEM-VIP250-128M-D=	128 Mbytes DRAM Option for VIP2-50/xIP-50
MEM-VIP250-4M-S=	4 Mbytes SRAM Option for VIP2-50/xIP-50 (default)
MEM-VIP250-8M-S=	8 Mbytes SRAM Option for VIP2-50/xIP-50

Cisco 7500 VIP4 Memory Options

MEM-VIP4-64M-SD=	64 MB SDRAM Option for VIP4 (Spare)
MEM-VIP4-128M-SD=	128 MB SDRAM Option for VIP4
MEM-VIP4-256M-SD=	256 MB SDRAM Option for VIP4

Cisco 7500 VIP6 Memory Options

MEM-VIP6-64M-SD=	64 MB SDRAM Option for VIP6 (Spare)
MEM-VIP6-128M-SD=	128 MB SDRAM Option for VIP6
MEM-VIP6-256M-SD=	256 MB SDRAM Option for VIP6

Cisco 7500 Series Memory Upgrades

VIP2-10/15/FE2-UPG	DRAM MEM Upgrade for VIP2-10, VIP2-15, CX-FEIP2-2TX AND -2FX
V2-10/15/FE2-UPG=	DRAM MEM Upgrade for VIP2-10, VIP2-15, CX-FEIP2-2TX AND -2FX

Cisco 7500 Series Port Adapters

PA-A3-OC12SMI=	1 Port ATM Enhanced OC12/STM4 single mode intermediate reach
PA-A3-OC12MM=	1 Port ATM Enhanced OC12/STM4 multi-mode
PA-A1-OC3SM	1 Port ATM OC3 Single Mode Intermediate Reach Port Adapter
PA-A1-OC3MM=	1-Port ATM OC3 Multimode Port Adapter
GEIP+=	Enhanced Gigabit Ethernet

Cisco7200, 7400 and 7500 Series Port Adapters[2]

Cisco7400 and 7500 Series Port Adapters[3]

Cisco 7500 Service Adapters

SA-ENCRYPT=	Encryption Service Adapter - Spare

Cisco 7500 Series CIP Options and Accessories

MEM-CIP-8M=	8 MB Memory, Replaces Existing CIP Memory, Total 8 MB
MEM-CIP-32M=	CIP 32 MB DRAM Upgrade Kit
MEM-CIP-64M=	CIP 64 MB DRAM Upgrade Kit
MEM-CIP-128M=	CIP 128 MB DRAM Upgrade Kit
FR-CIP-CSNA=	SNA SUPPORT FEATURE FOR CIP
FR-CIP-TCPOFF=	TCP/IP OFFLOAD FEATURE FOR CIP
FR-CIP-TN3270S-L=	TN3270 Server - Limited 2000 Session Support
FR-CIP-TN3270S-LS=	TN3270 Server - Limited 2000 Session Support SSL
FR-CIP-TN3270S-MS=	TN3270 Server - Mid-tier 5000 Session SupportSSL
FR-CIP-TN3270S-US=	TN3270 Server - Unlimited CIP2 Support SSL
FR-CIP-TNUPG-L-S=	TN3270 Server Upgrade 2,000 Sessions To SSL
FR-CIP-TNUPG-M-S=	TN3270 Server Upgrade 5,000 Sessions To SSL
FR-CIP-TNUPG-U-S=	TN3270 Server Upgrade Unlimited Sessions To SSL
FR-CIP-TNUPG-LM-S=	TN3270 Server Upgrade From 2,000 Sessions To 5,000 SSL
FR-CIP-TNUPG-MU-S=	TN3270 Server Upgrade From 5,000 Sessions To Unlimited SSL
FR-CIP1-TN3270S-G=	CIP1: TN3270 Server Upgrade, Limited to Unlimited Version
FR-CIP2-TN3270S-G=	CIP2: TN3270 Server Upgrade, Limited to Unlimited Version
FR-CIP2-TN3270S-M=	TN3270 Server - Mid-tier 5000 session support
FR-CIP1-TN3270S-U=	TN3270 Server - Unlimited CIP1 Support
FR-CIP2-TN3270S-U=	TN3270 Server - Unlimited CIP2 Support
FR-CIP1-TNUPG-G-S=	TN3270 Server upgrade, limited to unlimited version with SSL
FR-CIP2-TNUPG-G-S=	CIP2: TN3270 Server upgrade, limited to unlimited -SSL
FR-CIP2-TNUPG-LM=	TN3270 server upgrade from 2000 to 5000 sessions
FR-CIP2-TNUPG-MU=	TN3270 server upgrade from 5000 to unlimited sessions
FR-CIP-SNASWITCH=	TN3270 Server - SNA Session Switch Feature
FR-CIP-ASSIST	TCP Assist Feature on CIP for host using Cisco IOS for S/390

NetFlow Utility Software

NDA-HPUX-3.X-UPG	Upgrade To Analyzer 3.6 For HP U/X Incl NFC 3.5
NDA-SOSU-3.X-UPE	Upgrade To Analyzer 3.6 For Solaris Incl NFC 3.5
NDA-HPUX-3.X-UPE	Upgrade To Analyzer 3.6 For HP U/X Incl NFC 3.5

Cisco 7500 RSP Feature Licenses

FR-WPP75=	Cisco IOS RSPx Series WAN Packet Protocols/Netflow License
FR-IR75=	Cisco IOS RSP Series InterDomain Routing License
FR75-AN2=	Cisco IOS 7500 Series DBConn

Cisco 7500 Series IOS Feature Licenses

FR75-APPN=	Cisco IOS RSPx Series APPN Upgrade
FR75-BS-A=	Cisco IOS RSPx Series Desktop/IBM to Enterpise
FR75-C-DS=	Cisco IOS RSPx Series IP to IP/IPX/IBM
FR75-C-BS=	Cisco IOS RSPx Series IP to Desktop/IBM
FR75-C-A=	Cisco IOS RSPx Series IP to Enterprise
FR75-DS-BS=	Cisco IOS RSPx IP/IPX/IBM to Desktop/IBM
FR75-DS-A=	Cisco IOS RSPx IP/IPX/IBM to Enterprise
FR75-40=	Cisco IOS RSPx Encryption 40 Upgrade
FR75-56=	Cisco IOS RSPx Encryption 56 Upgrade
FL75-H=	Cisco IOS 7500 Series Firewall/IDS Upgrade
FL75-K2=	Cisco IOS 7500 Series IPSEC 3DES Upgrade
FL75-L=	Cisco IOS 7500 Series IPSEC 56 Upgrade
FL75-R1=	Cisco IOS RSPx Series SNASwitch Upgrade
FL75-N-R1=	Cisco IOS 7500 Series APPN to SNASwitch Upgrade
FR-ITP-HSL=	IP Transfer Point (ITP) High Speed Link (HSL) License

Cisco 7500 Series IOS Feature Set Upgrades

FR-ITP-M3UA/SUA=	IP Transfer Point M3UA/SUA Functionality License
FR-ITP-M2PA=	IP Transfer Point M2PA Functionality Feature License

Versatile Interface Processor Port Adapters (VIP2 and VIP4)

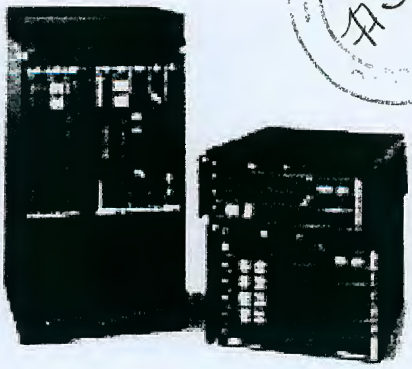
PA-MC-8TE1+=	8 port multichannel T1/E1 8PRI port adapter

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.
2. Cisco 7200, 7400 and 7500 share many port adapters. Please see Cisco 7200, 7400 and 7500 Series Port Adapters, page 1-34 for additional part numbers.
3. Cisco 7400 and 7500 share many port adapters. Please see Cisco7400 and 7500 Series Port Adapters, page 1-43 for additional part numbers.

For More Information

See the Cisco 7500 Series Web site: **http://www.cisco.com/go/7500**

Cisco 7600 Series



The Cisco 7600 Series combines optical WAN/MAN networking and high-volume Ethernet aggregation with a focus on line-rate delivery of high-touch IP services in large data centers and at the edge of service provider networks. It provides customers the flexibility of three different form factors: Cisco 7603, 7606, and 7609. As the most scalable system in the industry, each router offers the ability to deliver DS0 to OC-48 WAN connectivity, and 10-Mbps Ethernet to 10-Gigabit Ethernet LAN connectivity into Internet data center, metropolitan aggregation, WAN edge aggregation, and enterprise networking applications.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7603	• 3 slot (horizontal) chassis • 32 Gbps backplane bandwidth • 15 Mpps forwarding rate • NEBs Compliant
Cisco 7606	• 6 slot (horizontal) chassis • 160 Gbps backplane bandwidth • 30 Mpps forwarding rate • NEBs Compliant
Cisco 7609	• 9 slot (vertical) chassis • 256 Gbps backplane bandwidth • 30 Mpps forwarding rate • NEBs Compliant

Key Features

- Hardware accelerated IP services on each Optical Services Module (OSM), delivering up to 6 Mpps per slot
- 15 to 30 Mpps forwarding processor and up to 512 MB DRAM for Internet routing
- Modular and scalable from 32 Gbps to 256 Gbps switch fabric
- One of the widest, most complete ranges of WAN interfaces in the industry, with DS0 to OC-48 connectivity
- Leveraging the FlexWAN Module, 7x00 port adapters are shared with the Cisco 7200, 7300, 7400, and 7500 which simplifies sparing and protects customer investment in interfaces
- Compatible with Catalyst 6500 LAN interfaces, offering 10 Mbps Ethernet to 1 Gbps

Competitive Products

• Redback: SMS-500, SMS-1800	• Unisphere: ERX700, ERX1400
• Juniper: M5, M10, M20, M40	• Extreme: Black Diamond 6808

Specifications

Feature	Cisco 7603	Cisco 7606	Cisco 7609
Fixed Ports	None	Same as Cisco 7603	Same as Cisco 7603
Expansion Slots	3 (horizontal)	6 (horizontal)	9 (vertical)
WAN Interface Range	DS0 to OC-48	Same as Cisco 7603	Same as Cisco 7603
Processor	Supervisor Engine 2 w/MSFC2 and PFC2	Same as Cisco 7603	Same as Cisco7603
Forwarding Rate	Up to 15 Mpps	Up to 30 Mpps	Up to 30 Mpps
Backplane Capacity	32 Gbps	160 Gbps	256 Gbps
Flash PCMCIA Memory	16MB (expandable to 24MB)	Same as Cisco 7603	Same as Cisco 7603
System DRAM Memory	128MB (expandable to512MB)	Same as Cisco 7603	Same as Cisco 7603
Minimum Cisco IOS Release	12.1(8)AE3	Same as Cisco 7603	12.1(8)(A)EX
Internal Power Supply	AC or DC (1000 W)	AC or DC (1000 W)	AC or DC (1300 or 2500 W)
Redundant Power Supply Support	Yes	Same as Cisco 7603	Same as Cisco 7603
Chassis Height	4 RU	7 RU	20 RU
Rack Mountable	Yes, up to 10 per rack	Yes, up to 6 per rack	Yes, up to 2 per rack
Dimensions (HxWxD)	7 x 17.37 x 21.75 in.	12.25 x 17.37 x 21.75 in.	25.2 x 17.2 x 18.1 in.

Selected Part Numbers and Ordering Information[1]

Cisco 7609 Systems	
CISCO7609	7609 Chassis Bundles
7609-AC-BUN	Enhanced 7609 Chassis, SUP2/MSFC2, 4000W AC P/S, 512MB DRAM
7609-DC-BUN-2500W	Enhanced 7609 Chassis, SUP2/MSFC2, 2500W DC P/S, 512MB DRAM
OSR-7609-AC	7609 Chassis, SUP2/MSFC2, 2500W AC P/S, 512MB DRAM
OSR-7609-DC	7609 Chassis, SUP2/MSFC2, 2500W DC P/S, 512MB DRAM
Cisco 7606 Systems	
CISCO7606	Cisco 7606 Chassis Bundle
7606-AC-BUN	7606 Chassis, SUP2/MSFC2, 1900W AC P/S, PEM, 256MB DRAM
7606-DC-BUN	7606 Chassis, SUP2/MSFC2, 1900W DC P/S, PEM, 256MB DRAM
CISCO7606-CHASS	Cisco 7606 Chassis
Cisco 7603 Systems	
CISCO7603	Cisco 7603 Chassis Bundle
7603-AC-BUN	7603 Chassis, SUP2/MSFC2, 950W AC P/S, PEM, 256MB DRAM
7603-DC-BUN	7603 Chassis, SUP2/MSFC2, 950W DC P/S, PEM, 256MB DRAM
CISCO7603-CHASS	CISCO 7603 Chassis
Cisco 7600 Optical Services Modules (OSMs)	
DSM-1CHOC12/T1-SI=	1-port CHOC-12/CHSTM-4 OSM IR, to DS0 and T1/E1, w/4GE
DSM-12CT3/T1=	12-port Channelized DS-3 to DS-1/DS-0
OSM-1CHOC48/T3-SS=	1-port CHOC-48/CHSTM-16 OSM, to T3/E3, SM-SR, with 4 GE
OSM-1CHOC12/T3-SI=	1-port CHOC-12/CHSTM-4 OSM, to T3/E3, SM-IR, with 4 GE
OSM-1OC48-POS-SI=	1-port OC-48/STM-16 SONET/SDH OSM, SM-IR, with 4 GE
OSM-1OC48-POS-SL=	1-port OC-48/STM-16 SONET/SDH OSM, SM-LR, with 4 GE
OSM-1OC48-POS-SS=	1-port OC-48/STM-16 SONET/SDH OSM, SM-SR, with 4 GE
OSM-2OC12-ATM-MM=	2-port OC-12/STM-4 ATM OSM, MM, with 4 GE
OSM-2OC12-ATM-SI=	2-port OC-12/STM-4 ATM OSM, SM-IR, with 4 GE
OSM-2OC12-POS-MM=	2-port OC-12/STM-4 SONET/SDH OSM, MM, with 4 GE
OSM-2OC12-POS-SI=	2-port OC-12/STM-4 SONET/SOH OSM, SM-IR, with 4 GE
OSM-2OC12-POS-SL=	2-port OC-12/STM-4 SONET/SDH OSM, SM-LR, with 4 GE
OSM-4GE-WAN-GBIC=	4-port Gigabit EthernetOptical Services Module, GBIC
OSM-4OC3-POS-SI=	4-port OC-3/STM-1 SONET/SDH OSM, with 4 GE
OSM-4OC12-POS-MM=	4-port OC-12/STM-4 SONET/SDH OSM, MM, with 4 GE
OSM-4OC12-POS-SI=	4-port OC-12/STM-4 SONET/SDH OSM, SM-IR, with 4 GE
OSM-4OC12-POS-SL=	4-port OC-12/STM-4 SONET/SDH OSM, SM-LR, with 4 GE
OSM-8OC3-POS-MM=	8-port OC-3/STM-1 SONET/SDH OSM, MM, with 4 GE
OSM-8OC3-POS-SI=	8-port OC-3/STM-1 SONET/SDH OSM, SM-IR, with 4GE
OSM-8OC3-POS-SL=	8-port OC-3/STM-1 SONET/SDH OSM, SM-LR, with 4 GE
OSM-16OC3-POS-MM=	16-port OC-3/STM-1 SONET/SDH OSM, MM, with 4 GE
OSM-16OC3-POS-SI=	16-port OC-3/STM-1 SONET/SDH OSM, SM-IR, with 4 GE
OSM-16OC3-POS-SL=	16-port OC-3/STM-1 SONET/SDH OSM, SM-LR, with 4 GE
OSM-2OC48/1DPT-SS=	2-port OC-48/STM-16 POS/DPT OSM, SM-SR, with 4 GE
OSM-2OC48/1DPT-SI	2-port OC-48/STM-16 POS/DPT OSM, SM-IR, with 4 GE

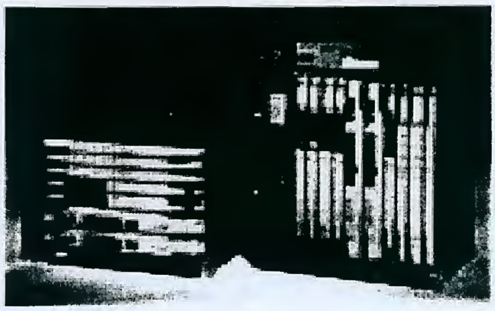
OSM-2OC48/1DPT-SL=	2-port OC-48/STM-16 POS/DPT OSM, SM-LR, with 4 GE
Cisco 7600 Line Cards	
WS-F6K-DFC=	Distributed Forwarding Card
WS-X6348-RJ-45=	Catalyst 6000 48-port 10/100, Upgradable to Voice, RJ-45
WS-X6516-GBIC=	Catalyst 6500 16-port GigE Mod: fabric-enabled (Req. GBICs)
WS-X6524-100FX-MM=	Catalyst 6500 24-port 100FX, MT-RJ, fabric-enabled
WS-X6502-10GE=	Catalyst 6500 10 Gigabit Ethernet Base Module(Req OIM),Spare
WS-X6816-GBIC=	Catalyst 6500 16-port GigE mod, 2 fab I/F w/DF, (Req GBICs)
WS-X6548-RJ-21=	Catalyst 6500 48-port 10/100, RJ-21, fabric-enabled
WS-X6548-RJ-45=	Catalyst 6500 48-port 10/100, RJ-45, x-bar
WS-X6516-GE-TX=	Catalyst 6500 16-port Gig/Copper Module, x-bar
Cisco 7600 Memory Options	
MEM-OSM-64M=	64MB ECC Memory for Optical Services Modules
MEM-OSM-128M	128 MB ECC Memory for Optical Services Modules
MEM-OSM-256M	256 MB ECC Memory for Optical Services Modules
MEM-OSM-512M	512 MB ECC Memory for Optical Services Modules

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 7600 Series Web site: **http://www.cisco.com/go/7600**

Cisco 10000 Series



The Cisco 10000 Series is the industry's only edge router that delivers consistent, high performance services for carriers deploying IP, MPLS, and broadband services to DSL and private line customers. Coupled with proven high availability and innovative adaptive network processing technology, the Cisco 10000 Series is uniquely designed to meet the service needs of carriers up to DS3/E3 aggregation speeds.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 10008	• Broadband features including PPP over ATM, PPP over Ethernet, routed bridge encapsulation, and Layer 2 Tunneling Protocol • MPLS, MPLS VPN, and MPLS Quality of Service edge features • Leased line features such as seamless integration from a dedicated access environment (TDM or SONET/SDH) to the ATM core.

Key Features

- Industry-leading high availability—nonstop performance, with a complete set of reliability features for high availability (99.999 percent uptime). Full hardware redundancy, hot-swappable elements, and seamless route processor cutover provide continuous traffic forwarding.
- Lowest total cost of ownership—the Cisco 10000 offers the highest leased-line, ATM, frame, and broadband session densities on a single platform, and its high reliability reduces network downtime and operational expenses
- Broad portfolio of line-rate IP sessions—critical service features, such as QoS, MPLS, Multilink PPP, and ACLs are hardware accelerated to deliver exceptional throughput for every connection

- Industry-leading session density—the Cisco 10000 supports thousands of DS0, DS1/E1 connections, or hundreds of clear-channel DS3 connections on a single platform, providing the highest port density of DS3-and-below interfaces

Competitive Products

- Redback: SMS-10000
- Juniper: M5, M10, M20
- Unisphere: ERX700, ERX1400

Specifications

Feature	Cisco 10008
Fixed Ports	None
Expansion Slots	8 (for interfaces)
WAN Interface Range	DS0 to OC-12
Processor	Cisco PXF Processor
Forwarding Rate	10005Up to approximately 6 Mpps
Backplane Capacity	51.2 Gbps
Flash PCMCIA Memory	48 MB (expandable to 128 MB)
System DRAM Memory	512 MB
Minimum Cisco IOS Release	12.0(9)SL
Internal Power Supply	AC or DC, dual option
Redundant Power Supply	Yes, for both AC and DC
Chassis Height	13 RU
Rack Mountable	Yes, up to 3 per rack
Dimensions (HxWxD)	21.75 x 17.5 x 12 in.

Selected Part Numbers and Ordering Information[1]

Cisco 10008 Pricing Bundles	
ESR10008-1P1AC	C10000 8-slot chassis,1 PRE, 1 AC PEM
ESR10008-1P1AC+6	C10000 8-slot chassis,1 PRE, 1 AC PEM,1CT3 module
ESR10008-1P1DC	C10000 8-slot chassis,1 PRE, 1 DC PEM
ESR10008-1P1DC+6	C10000 8-slot chassis,1 PRE, 1 DC PEM,1CT3 module
ESR10008-1P1AC+4CH	C10000 8-slot chassis, 1 PRE, 1 AC PEM, 1 CH STM-1 Module
ESR10008-1P1DC+4CH	C10000 8-slot chassis, 1 PRE, 1 DC PEM, 1 CH STM-1 Module
ESR10008-2P2AC	C10000 8-slot chassis,2 PREs, 2 AC PEMs
ESR10008-2P2AC+6	C10000 8-slot chassis,2 PREs, 2 AC PEMs,1 CT3 module
ESR10008-2P2DC	C10000 8-slot chassis,2 PREs, 2 DC PEMs
ESR10008-2P2DC+6	C10000 8-slot chassis,2 PREs, 2 DC PEMs,1 CT3 module
ESR10008-2P2AC+4CH	C10000 8-slot chassis, 2 PREs, 2 AC PEMs, 1 CH STM-1 Module
ESR10008-2P2DC+4CH	C10000 8-slot chassis, 2 PREs, 2 DC PEMs, 1 CH STM-1 Module
ESR10008-1P1DC-SK	ESR10008 BBA Starter Kit with PRE1, DC, 4-port OC3, GE
Cisco 10005 Pricing Bundles	
ESR10005-1P1AC	C10000 5-slot chassis, 1 PRE, 1 AC PEM
ESR10005-1P1DC	C10000 5-slot chassis, 1 PRE, 1 DC PEM
ESR10005-1P1AC+6	C10000 5-slot chassis, 1 PRE, 1 AC PEM, 1 CT3 Module
ESR10005-1P1DC+6	C10000 5-slot chassis, 1 PRE, 1 DC PEM, 1CT3 Module
ESR10005-1P1AC+4CH	C10000 5-slot chassis, 1 PRE, 1 AC PEM, 1 CH STM-1 Module
ESR10005-1P1DC+4CH	C10000 5-slot chassis, 1 PRE, 1 DC PEM, 1 CH STM-1 Module
ESR10005-2P2AC	C10000 5-slot chassis, 2 PREs, 2 AC PEMs
ESR10005-2P2DC	C10000 5-slot chassis, 2 PREs, 2 DC PEMs
ESR10005-2P2AC+6	C10000 5-slot chassis, 2 PREs, 2 AC PEMs, 1CT3 Module
ESR10005-2P2DC+6	C10000 5-slot chassis, 2 PREs, 2 DC PEMs, 1CT3 Module
ESR10005-2P2AC+4CH	C10000 5-slot chassis, 2 PREs, 2 AC PEMs, 1 CH STM-1 Module
ESR10005-2P2DC+4CH	C10000 5-slot chassis, 2 PREs, 2 DC PEMs, 1 CH STM-1 Module
ESR10005-CHAS=	C10000 5-SLOT CHASSIS, INCL 5xDS3 EXT CRD,ALM CRD,BWR,SPARE
ESR-PRE1	Performance Routing Engine, 512 DRAM and 32M Flash

Cisco 10000 Series Memory Options

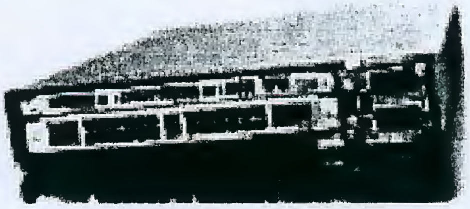
ESR-PRE-MEM-FD48	C10000 PRE 48M Flash Disk (default)
ESR-PRE-MEM-FD128	C10000 PRE 128M Flash Disk option
ESR10005-PWR-AC	AC Power Entry Module
ESR10005-PWR-DC	DC Power Entry Module
ESR-PWR-DC=	DC POWER ENTRY MODULE FOR ESR10008
ESR-PWR-AC	AC power entry module for ESR10008
ESR-PWR-AC/R	Redundant AC powerentry module for ESR10008,spare
ESR10005-PWR-AC=	AC POWER ENTRY MODULE, SPARE
ESR10005-PWR-AC/R	Redundant AC Power Entry Module
ESR10005-PWR-DC/R	Redundant DC Power Entry Module
CAB-DS-ACE	Power Cables for AC Power Option, European
CAB-DS-ACI	Power Cables for AC Power Option, Italian
CAB-DS-ACJ-TWLK	Power Cables for AC Power Option, Japan
CAB-DS-ACU	Power Cables for AC Power Option, UK
CAB-DS-120VAC	Cisco 120 VAC Power Cable, US
ESR-24CT1/E1	24port Channelized E1/T1 Line Card
ESR-8E3/DS3	8 port clear channelE3/DS3 Line Card
ESR-6CT3	6 port channelized T3line card
ESR-1GE	1 pt Gigabit Ethernet line card (requires a GBIC)
ESR-GBIC-SX	1000base-SX GBIC, multimode,standardized forESR
ESR-GBIC-LHLX	1000base-LH GBIC,singlemode,standardizedfor ESR
ESR-GBIC-ZX	1000base-ZX GBIC,singlemode,standardized for ESR
ESR-4OC3ATM-SM	4 Port OC3/STS3c/STM1c ATM Line Card, single mode
ESR-1COC12-SMI	1 pt ChOC12 (STS12) line card, single mode intermed. reach
ESR-1OC12/P-SMI	1 pt OC12/STS12c/STM4 POS, single mode, int reach
ESR-1OC12ATM-SM	1 pt OC12/STM4 ATM Line Card, Single-Mode

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 10000 Series Web site: **http://www.cisco.com/go/10000**

Cisco 10720 Series



The Cisco 10720 Internet Router is a high-performance router and a principle building block in the metro IP network. It enables service providers to offer innovative and differentiated IP services to their customers at optical speeds. Equipped with Ethernet technology for customer access and the innovative Dynamic Packet Transport (DPT)/RPR (Resilient Packet Ring) technology or Packet over SONET (POS) for metro optical connectivity, the Cisco 10720 allows service providers to offer IP services closer to the user, enabling them to better control admission to network resources. This allows service providers to bypass traditional DS1 and DS3 access options. The dual counter rotating ring technology of DPT is also cost effective, since it uses both rings and can be deployed over dark fiber and still maintain the less than 50ms restoration common in SONET/SDH systems. For multiservice applications, DPT can also be deployed over traditional SONET/SDH ADMs and wavelength division multiplexing (WDM) systems.

The Cisco 10720 is a cost-effective, reliable platform that not only supports the full suite of IP routing protocols such as IS-IS, OSPF and BGP, but also allows advanced IP features to be introduced efficiently, without compromising on performance. Although primarily designed for high-speed Internet services for multitenant and business-park applications in the metro, the Cisco 10720 Internet Router is also suitable for a range of other applications such as: Internet data center applications, intra-POP aggregation, cable multisystem operator (MSO) internetworking, and voice-over-IP (VoIP) aggregation.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 10720 Internet Router	• Any service provider planning to offerhigh-performance IP services as part of their business strategy by extending IP further out into the network • Any service provider wanting to simplify their current network and implement thesimple, scalable, reliable features of DPT technology while maximizing fiber usage • Any customer already using DPT technology in their network, most likely with DPT cards on the 12000 Internet Router • Metro Ethernet Servicessuch as L2 and L3 VPN with FE/GE handoff to the Customer and 50ms restoration overdark fiber using DPT.

Key Features

- Equipped with Redundant Power Supply by default
- SRP specific features—IPS with <50 ms restoration time and SRP MIB support
- Multicast support including PIM SM, PIM DM, MBGP
- L2 VPN—UTI, L2TPv3 and EoMPLS for Layer 2 to Layer 2 LAN extension; L3 VPN MPLS VPN
- QoS—Modular QoS CLI, CAR, WRED, VTMS traffic shaping, and access lists
- Ethernet features—MDI-MDI-X support, 10/100 speed auto-negotiation, HDX-FDX negotiation and time delay reflectometry (TDR) for 10/100BaseTX
- Hot Standby Routing Protocol (HSRP)/Multiple Hot Standby Routing Protocol (MHSRP)
- 64-MB built-in Flash for software and configuration load
- Optical receive power monitoring support on OC-48/STM-16 Interface and GE
- Supported management information bases (MIBs) include SNMP, SRP, SONET, Etherlike, OSPF

Competitive Products (vs. Cisco's Metro IP RPR Solution using the 10720)

- Extreme Summit: 48/Blackdiamond comb for GigE Hub & Spoke
- Riverstone: RS3000/RS8600 combo for GigE Hub & Spoke

Specifications

Feature	Cisco 10720
Security Features	Including AAA, RADIUS authentication, TACACS+, and encrypted passwords
Management	Cisco IOS CLI TACACS+ and RADIUS Configuration and administration features including Telnet and CiscoDiscovery Protocol (CDP) Serial (aux) and consoleports for local and remote administration Remote software download via TFTP and RCP IP over DCC for remote management of the Cisco ONS 15104 OC-48/STM-16 Optical Regenerator, where applicable
Physical Interfaces	Uplink Modules: 2-port single-mode OC-48c/STM16c DPT (SR 2 km (1.2 miles), IR 15 km (9.3 miles), LR1 40km (24 miles) and LR2 80km (50miles) Interface Modules—The Cisco 10720 Internet Router has two dedicated slots for interface modules—modulesare not interchangeable or hot swappable: • Upper slot is dedicated for DPT or POS Uplink module equipped withtwo physical ports of OC-48c/STM16c that provide an aggregate bandwidth of approximately 5 Gbps. The cards are available in two four versions of optics, short reach (SR) and intermediate reach (IR), Long Reach1 (LR1) and Long Reach2 (LR2) with two small form-factor OC-48 ports with LC connectors • A third option for the upperslot is the CON-AUX module, which is a depopulated uplinkcard equipped with Console and Auxiliary ports only; this allows the configuration of the 10720 as an "Ethernet Router" allowing the use of one or more of the Ethernet ports in the lower slot for network connectivity • Lower slot is dedicated for24-port Fast Ethernet module—available in TX (100 m reach), FX-MM (2 km reach) or FX-SM (15 km reach). The TX module is equipped with RJ-45 connectorswhile the FX-SM and FX-MM modules are equipped with MT-RJ connectors. • Also available is a combination 4 Gigabit Ethernetwith Small Form Factor Plug-able (SFP) Optics available in SX 550m and LH 10km plus an additional 8 Ports of Fast Ethernet 10/100 TX Copper ports. The TX and the FX-MM versions of the 24-port Fast Ethernet modules accommodate copper or multimode fiber deploymentswithin MTUs and the FX-SM allows for deployment of the Cisco 10720 Internet Router in a central location covering Ethernet connectivity to buildings for a radius of up to 15 km.
Dimensions	3.5 x 17.25 x 18.25 in. (8.9 x 43.81 x 46.35 cm)

Selected Part Numbers and Ordering Information[1]

Cisco 10700 Series

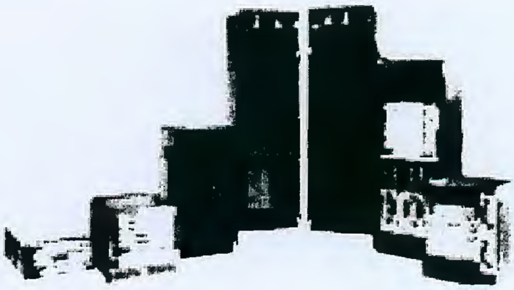
CISCO10720-AC-A	Cisco 10720 Internet Router with dual AC power supply
CISCO10720-DC-A	Cisco 10720 Internet Router with dual DC Power Supply
10720-FE-TX	24-port 10/100 Ethernet Access Module—RJ45 connectors
10720-FE-FX-MM	24-port 100Mbps Multimode Fiber Ethernet Access Module 2km—MTRJ connectors
10720-FE-FX-SM	24-port 100Mbps Single mode Fiber Ethernet Access Module 15km—MTRJ connectors
10720-GE-FE-TX	4-port 100Mbps SFP GE with 8-ports of 10/100 Ethernet TX-RJ45
10720-SR-LC	OC-48c/STM-16c SRP Short Reach (2km) Uplink Module—LC connectors
10720-IR-LC	OC-48c/STM-16c SRP Intermediate Reach (15km) Uplink Module—LC connectors
10720-LR1-LC	OC-48c/STM-16c SRP Long Reach 1 (40km) Uplink Module — LC
10720-LR2-LC	OC-48c/STM-16c SRP Long Reach 2 (80km) Uplink Module-LC connectors
10720-CON-AUX	Console and Auxiliary port that fits in the Upper Slot
10720-SR-LC-POS	OC-48c/STM-16c POS Short Reach (2km) Uplink Module-LC connectors
10720-IR-LC-POS	OC-48c/STM-16c POS Intermediate Reach (15km) Uplink Module-LC connectors
10720-LR1-LC-POS	OC-48c/STM-16c POS Long Reach 1 (40km) Uplink Module - LC
10720-LR2-LC-POS	OC-48c/STM-16c SRP Long Reach 2 (80km) Uplink Module-LC connectors

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 10720 Internet Router Web site: **http://www.cisco.com/go/10700**

Cisco 12000 Series



The Cisco 12000 Series Internet Router is part of Cisco's family of multimillion packets-per-second (mpps) IP and MPLS routing platforms for building profitable networks in today's communications economy. The Cisco 12000 Series is the premier high-end routing platform for service provider backbone and edge applications, enabling service providers to meet the challenge of building packet networks to satisfy services demand while increasing profitability. The Cisco 12000 Series offers the only portfolio of 10 Gbps per slot systems and interfaces (including Packet over SONET [POS], Dynamic Packet Transport/Resilient Packet Ring [DPT/RPR], and Gigabit Ethernet [GbE]), delivering 10G economies of scale anywhere in the network. The Cisco 12000 Series provides the highest reliability, the richest set of service enablers, the lowest total cost of ownership, and the only proven investment protection, including systems that can be upgraded in the field to increase switching capacity. This innovative combination of features and capabilities enables service providers to build the most competitive IP and MPLS networks.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 12400 Internet Routers (10G)	• 10 Gbps/slot, from 80 to 320 Gbps of non-blocking switching capacity • Supportfor high-density, high-speedinterfaces: ATM, DPT/RPR, POS, GbE/FE ranging from channelized DS3 (to DS1) throughOC-192c/STM-64c • 4 10G platforms to choose from: 12416, 320 Gbps, 16 slots, 40 RU; 12410, 200 Gbps, 10 slots, 20 RU; 12406, 120 Gbps, 6 slots, 10 RU; 12404, 80 Gbps, 4 slots, 5 RU • Support for industry-leading QoS/CoS featuresideal for peering, transit, POP consolidation, and IDC bandwidth aggregation as well as latency-sensitive applicationslike voice and video • Support for IP or MPLS forwarding • Support for hundredsof thousandsof routes • Proven carrier- class reliabilityand availability throughenhancedfeatures such as Online Insertion and Removal, High Availability (RPR+, NSF and SSO) and APS/MPS
Cisco 12000 Internet Routers (2.5G)	• 2.5 Gbps/slot, from 40 to 80 Gbps switching capacity • Supportfor high-density, high-speedinterfaces: ATM, DPT/RPR, POS, GbE/FE ranging from channelized DS3 (to DS1) throughOC-48c/STM-16c • 3 chassis to choose from: 12016, 80 Gbps, 16 slots, 40 RU; 12012, 60 Gbps, 12 slots, 32 RU; 12008, 40 Gbps, 8 slots, 14 RU • The 12016 InternetRouter is upgradeableto 320 Gbps via an easy, field-installed switch fabric upgrade kit—no need to pull out existing line cards
Cisco 12000 Manager	• An element management solutionto increase service velocity and decrease operation costs

Key Features

- Proven investment protection, offering full forward compatibility for all line cards, and the only high-end system with a modular, replaceable switch fabric for field-installed capacity upgrades
- Only fully distributed system architecture scales to the edge, supporting backbone- or edge-optimized line cards in the same chassis
- Only platform that maximizes the value of line-rate edge applications with 10G uplinks. By deploying Cisco 12000 Series IP Services Engine (ISE) line cards in Cisco 12400 Internet Routers, Service Providers benefit from line cards optimized for edge applications, while removing the bandwidth bottleneck with full 10 Gbps uplinks using cost-effective VSR optics or 10 GbE for intra-POP connections.
- The only complete priority packet delivery solution set
- Industry's only complete IP QoS and congestion control implementation that uniquely enables premium real-time services such as VoIP and video. Its distributed architecture and class of service features such as priority based congestion control (WRED) and dedicated low latency queuing (MDRR), along with virtual output queuing (VoQ), eliminate head of line blocking (HOL) and maintain packet sequence integrity under all conditions
- Non-service—impacting online insertion and removal (OIR) of components (including switch fabric cards) and front accessibility reduce downtime and simplify maintenance
- High availability features such as Cisco Non Stop Forwarding (NSF) and Cisco Stateful Switchover (SSO) eliminate single points of failure, help maintain system performance, and prevent service interruption. With these features, packet forwarding remains uninterrupted before, during and after a route processor switchover on the Cisco 12000 Series. Coupled with OIR, the faulty route processor can be replaced without affecting operation
- Designed for NEBS compliance to meet service provider carrier-class requirements

Competitive Products

- Juniper: T640, M160, M40E, M40, and M20
- Avici: Stackable Switch Router (SSR)

Specifications

Feature	Cisco 12008	Cisco 12012	Cisco 12016	Cisco 12404	Cisco 12406	Cisco 12410	Cisco 12416
Switching Capacity	40 Gbps	60 Gbps	80 Gbps	80 Gbps	120 Gbps	200 Gbps	320 Gbps
Capacity per slot (full duplex)	2.5 Gbps	2.5 Gbps	2.5 Gbps	10 Gbps	10 Gbps	10 Gbps	10 Gbps[1]
Chassis Size	1/3 Rack	Full Rack	Full Rack	1/8 Rack	1/4 Rack	1/2 Rack	Full Rack
Chassis Slots	8	12	16	4	6	10	16
Supported Line Cards	All Cisco 12000 Series 2.5 Gbps line cards See Part Numbers and Ordering Information	Same as Cisco 12008	All 2.5 Gbps line cards plus all 10 Gbps line cards when upgraded	Same as Cisco 12416	Same as Cisco 12416	Same as Cisco 12416	All Cisco 12000 Series Line Cards
Supported Protocols	IPv4, MPLS, BGPv4, IS-IS, OSPF v. 2.0, EIGRP, RIP v2, IGMP, PIM (dense and sparse mode)	Same as Cisco 12008	Same as Cisco 12008	Same as Cisco 12416	Same as Cisco 12416	Same as Cisco 12416	IPv4, MPLS, BGPv4, IS-IS, OSPF v. 2.0, EIGRP, RIP v2, IGMP,DVMRP, PIM DM/SM
Management	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager	CLI, SNMP, Cisco 12000 Manager
Dimensions	24.85 x 17.4 x 21.2 in. (63.1 x 44.2 x 53.8 cm)	56 x 17.3 x 21 in. (142.2 x 43.9 x 53.3 cm)	72.5 x 18.75 x 24 in. (184.2 x 47.6 x 61 cm)[2]	8.75 x 18.9 x 27.5 in. (22.23 x 48.01 x 69.85 cm)	18.5 x 18.9 x 28 in. (47 x 48 x 71.1 cm)[3]	37.5 x 19 x 24 in. (95.25 x 48.26 x 61 cm)[4]	72.5 x 18.75 x 24 in. (184.2 x 47.6 x 61 cm)[2]

1. The Cisco 12016 may be field upgraded to a Cisco 12416 via a Switch Fabric Upgrade kit, providing 10 Gbps full duplex capacity per slot, for an overall 320 Gbps switching capacity
2. Includes power, front cover, rack mount flanges, and cable-management system
3. Includes rack-mount flanges, power entry module pullouts, blower, and handle
4. Includes cable-management system and front cover

Selected Part Numbers and Ordering Information[1]

Cisco 12000 Series of Gigabit Switch Routers (GSR)	
GSR6/120-AC	GSR6/120 w/ 1GRP, 3SFC, 1 CSC, 2Alarms & 1 AC Power Supply
GSR6/120-DC	GSR6/120 w/ 1GRP, 3SFC, 1 CSC, 2Alarms & 1 DC Power Supply
GSR8/40	Cisco12008 GSR 40Gbps;1GRP,1CSC-GSR8,3SFC-GSR8,1DC
GSR10/200-AC	Cisco 12410 200 Gbps; 1GRP, 2 CSC, 5 SFC, 2 Alarm, 2 AC
GSR10/200-DC	Cisco 12410 200 Gbps; 1GRP, 2 CSC, 5 SFC, 2 Alarm, 2 DC
GSR12/60	Cisco12012 GSR 60Gbps;1GRP,1CSC,3SFC,1DC
GSR4/80-AC	GSR12404- 4 slot AC System
GSR4/80-DC	GSR12404- 4 slot DC System
GSR16/80-AC-8R	Cisco 12016 80 Gpbs; 1GRP, 2CSC, 3SFC, 2Alarm, 3AC, 8Rails
GSR16/80-AC4-8R	Same As GSR16/80-AC-8R But W/ 4AC And Requires 8 Foot Rack
GSR16/80-DC-8R	Cisco 12016 80 Gpbs; 1GRP, 2CSC, 3SFC, 2Alarm, 4DC, 8Rails
GSR16/320-AC	Cisco 12416 320 Gbps; 1GRP, 2CSC, 3SFC, 2Alarm, 3AC, 8Rails
GSR16/320-AC4	Same As GSR16/320-AC-8R But W/ 4 AC And Requires 8 Foot Rack
GSR16/320-DC	Cisco 12416 320 Gbps; 1GRP, 2CSC, 3SFC, 2Alarm, 4DC, 8Rails
Cisco 12000 Series Processors	
GRP-B	Route Processor, 128MB and 20MB Flash, ECC support
GRP-B/R	GSR Route Processor, Redundant Option
PRP-1	Cisco 12000 Series Performance Route Processor
PRP-1/R	Redundant PRP-1 chassis upgrade option, factory only

Cisco 12000 Series Line Cards

LC-4OC3/POS-SM	4port OC3/STM1 Packet Over SONET/SDH Line Card, Single-Mode
LC-4OC3/POS-MM	4port OC3/STM1 Packet Over SONET/SDH Line Card, Multi-Mode w
LC-1OC12/POS-SM	1port OC12/STM4 Packet Over SONET/SDH Line Card,Single-Mode
LC-1OC12/ATM-MM	1 port OC12/STM4 ATM Line Card, Multi-Mode
LC-1OC12/ATM-SM	1 port OC12/STM4 ATM Line Card, Single-Mode
LC-1OC12/POS-MM	1 port OC12/STM4 Packet Over SONET/SDH Line Card, Multi-Mode
CHOC48/DS3-SR-SC	1 port channelized oC-48to DS3
2CHOC3/STM1-IR-SC	Channelized OC3/STM1 -> DS1/E1, 2 ports Intermediate Reach
4CHOC12/DS3-I-SCB	4 PORT CHANNELIZED OC12 B
4OC3/ATM-IR-SC	4 port OC3/STM1 ATM Line Card intermediate reach
4OC3/ATM-MM-SC	4 port OC3/STM1 multimode ATM line card
4OC3/POS-LR-SC	4 port OC-3/STM1 SONET/SDH Long Reach LC with SC connector
4OC12/ATM-IR-SC	4 port OC-12/STM4 ATM LC Intermediate Reach
4OC12/ATM-MM-SC	4 port OC-12/STM4 ATM Line Card multimode
4OC12/POS-MM-SC-B	4OC12/POS-MM-SC-B
4OC12X/POS-M-SC-B	4-port OC12/POS Eng3 Multi-mode
4OC12/POS-IR-SC-B	4OC12/POS-IR-SC-B
4OC12X/POS-I-SC-B	4 PORT OC12 POS B
4OC48/SRP-SFP=	4 Port OC48c/STM16c SRP Linecard, SFP Optics
4OC48E/POS-LR-SC	Edge 4 Port OC-48c/STM-16c SONET/SDH LR with SC
4OC48E/POS-SR-SC	Edge 4 Port OC-48c/STM-16c SONET/SDH SR with SC
8OC03/ATM/TS-IR-B	8-port OC03/STM1 ATM IR LC with SC connector
8OC03/ATM/TS-MM-B	8-port OC03/STM1 ATM MM LC with SC Connector
OC12/SRP-IR-SC-B	OC12 SRP IR line card
OC12/SRP-LR-SC-B	OC12 SRP LR line card
OC12/SRP-MM-SC-B	OC12 SRP MM line card
OC12/SRP-XR-SC	OC12 SRP single ring linecard, single mode 1550, XR
OC48/SRP-LR-SC-B=	OC48 SRP Rev-B Line Card, Single Mode, Long Reach
OC48/SRP-SR-SC-B=	OC48 SRP Rev-B Line Card, Single Mode, Short Reach, GSR
OC48E/POS-LR-SC-B=	1 Port OC-48c/STM-16c SONET/SDH 1550nm LR with SC
OC48E/POS-SR-SC-B=	1 Port OC-48c/STM-16c SONET/SDH 1310nm SR with SC, GSR
OC48X/POS-LR-SC	CONCATENATED OC48 WITH EXTENDED FEATURES LONG REACH
OC48X/POS-SR-SC	1 port OC48 POS Extended features
8OC3/POS-MM=	8 port OC3/STM1 SONET/SDH Multi-Mode LC with MTRJ conn Spare
8OC3/POS-SM=	8 port OC3/STM1 SONET/SDHSingle-Mode LC with LC conn Spare
1X10GE-LR-SC=	Cisco 12000 1-Port 10GE Card, 1310nm serial, 10km, SC
16OC3/POS-MM=	16 port OC3/STM1 SONET/SDH Multi-Mode LC with MTRJ conn
16OC3/POS-SM=	16 port OC3/STM1 SONET/SDH Single-Mode LC with LC conn Spare
16OC3X/POS-I-LC-B	16 PORT OC3 WITH EXTENDED FEATURES RELEASE B
EPA-GE/FE-BBRD	Cisco 12000 Modular GE Baseboard w/ 1GE and 3 EPA Slots
EPA-3GE-SX/LH-LC	Cisco 12000 3-Port GE Port Adapter for EPA-GE/FE-BBRD
3GE-GBIC-SC	GSR12000 three-port GE line card
GE-GBIC-SC-B	GSR12000 single port Gigabit Ethernet line card
GBIC-SX-MM	1000base-SX GBIC module, multimode,standardized for GSR12000
GBIC-LH-SM	1000base-LH GBIC module,singlemode,standardized for GSR12000
GBIC-ZX-SM	GBIC very long reach GBIC module for the GE line card
6CT3-SMB	Channelized T3for the GSR
GLC-LH-SM	GE SFP, LC connector LHtransceiver
GLC-SX-MM	GE SFP, LC connector SXtransceiver
6DS3-SMB-B	6DS3-SMB-B w/ ECC
6E3-SMB	E3 line card, 6 ports
12DS3-SMB-B	12DS3-SMB-B w/ ECC
12E3-SMB	E3 line card, 12 ports
CHOC12/STS3-IR-SC=	Channelized OC-12/STM-4 with four STS-3c/STM-1 POS paths
LC-OC12-DS3	1 port Channelize OC-12 with 12 DS3s
8FE-FX-SC-B	GSR 8-port 100baseFX, SC connector, version B
8FE-TX-RJ45-B	8-port 100baseTX, RJ45 connectortype, version B
OC192/POS-IR-SC	1 Port OC192c/STM64c POS, 1550nm IR, SC
OC192/POS-SR-SC	1 Port OC192c/STM64c POS, 1310nm SR, SC
OC192/POS-VSR	1 Port OC192c/STM64c POS, VSR Optics
OC192E/POS-VSR	1 Port OC192c/STM64c POS Edge Card, VSR Optics
OC192E/POS-IR-SC	1 Port OC192c/STM64c POS Edge Card, 1550nm IR, SC
OC192E/POS-SR-SC	1 Port OC192c/STM64c POS Edge Card, 1310nm SR, SC
OC192/SRP-VSR	1 Port OC192c/STM64c SRP Linecard, 850nm VSR, MTP
OC192/SRP-IR-SC	1 Port OC192c/STM64c SRP Linecard, 1550nm IR, SC
OC192/SRP-SR-SC	1 Port OC192c/STM64c SRP Linecard, 1310nm SR, SC

4GE-SFP-LC=	4 port-GE line card for Cisco 12000
Cisco 12000 Series Pluggable Optic Modules	
POM-OC48-LR2-LC	1-port OC-48/STM-16 Pluggable Optic Module, 1550nm SM-LR2 LC
POM-OC48-SR-LC	1-port OC-48/STM-16 Pluggable Optic Module, 1310nm SM-SR LC

1. Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 12000 Series Web site: **http://www.cisco.com/go/12000**

Cisco SN 5400 Series Storage Router

The Cisco SN 5400 Series implements the iSCSI protocol to extend access of a Fibre Channel fabric and attached storage devices to IP servers. iSCSI (internet SCSI) combines the benefits of the TCP/IP protocol suite with SCSI, the universal standard for storage access. By utilizing iSCSI, the SN 5400 Series extends a Fibre Channel storage network to lower priced/lower performance servers in a data center and departmental servers located throughout the campus and enterprise. With the SN 5428, access to a Fibre Channel Storage Area Network (SAN) from anywhere on an IP network is as easy as accessing direct attached storage.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco SN 5428	• When a customer is moving from a DAS (Direct Attached Storage) environment to a SAN (Storage Area Network) and they do not already have a Fibre Channel switch, the SN 5428 provides a Fibre Channel switch and iSCSI ports to deliver a one system solution. • When the customer wants only a full function Fibre Channel switch, the SN 5428 is a very cost effective, low latency switch that will perfectly fit a Fibre Channel only implementation • When the customer has block level applications and wants to maintain block level access to shared storage combined with IP/Ethernet for a substantial reduction in attachment costs

Key Features

- Provides levels of security and access control beyond what is currently available in traditional storage area networks by including layer 2 and layer 3 protection to resist against unauthorized access to your storage resources
- Uses the TCP/IP protocol suite for storage networking which protects your existing investment in storage and networking infrastructure
- Fully integrates existing management and configuration tools
- Based on industry standards, maximizes your investment and enables you to reduce total cost of ownership for the increasing storage demands on your network
- Uniquely provides standard IP networking capabilities to storage environments
- SN 5428: Designed for high-availability providing continuous access to critical data; Extensive security features to protect valuable storage resources; and, Full breadth of iSCSI drivers

Competitive Products

- Nishan
- McData: Fibre Channel Switches
- Qlogic: Fibre Channel Switches
- FalconStor
- Brocade: Fibre Channel switches

Selected Part Numbers and Ordering Information[1]

Cisco SN 5428 Storage Router	
SN5428	The SN 5428 provides two Gigabit Ethernetports, supporting iSCSI, for connection to sandard IP networks and eight Fibre Channel fabic switch ports.
Cisco SN 5428 Drivers & Firmware	
SN5428-FW-2.x	Cisco SN 5428 Firmware: 2.2.x minimum (2.2.1 minimum)
SN-ISCSI-DRV=	Cisco iSCSI drivers that support the Cisco SN 5428 2.2.x firmware: Windows NT, Windows 2000, Linux, Solaris, HP/UX, AIX
Cisco SN 5428 SFP: Small Form Factor Pluggables	
SN-SFP-FCMM-LC=	SFP for Fibre Channel Multi-mode fiber with LC connector
SN-SFP-FCMM-LC=	SFP for Fibre Channel Multi-mode fiber with connector spare
SN-SFP-FCGEMM-LC	SFP for GE/FC with LC connector
SN-SFP-FCGEMM-LC=	SFP for GE/FC with LC connector
Cisco SN 5420 Series Packaged SMARTnet Maintenance 8x5xNBD	
CON-SNT-PKG10	Cisco SN 5428 Packaged SMARTnet 8x5xNBD—Category 10

For More Information

See the Cisco SN5420 Series Storage Router Web sites:
http://www.cisco.com/go/sn5428

CHAPTER 2

LAN Switching

LAN Switching Products at a Glance

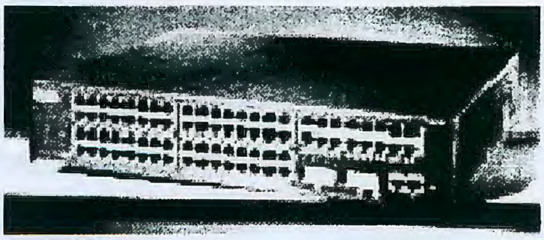
Product	Features	Page
Catalyst 2900 Series	Fixed-configuration Ethernet switches • 10/100 auto sensing and auto negotiating interface • Managed	2-3
Catalyst 2948G-L3	Fixed and Modular ports • Gigabit Ethernet over Fiber or Copper • High performance, Cisco Express Forwarding (CEF) Layer 2/3/4 switching up to 48 Mpps • Advanced network control with predictable performance, granular QoS, advanced security, comprehensive management	2-3
Catalyst 2900 Series XL—Modular Switches	Modular 10/100 Ethernet switches • 12 or 24 10/100 ports • 12 100BASE- FX ports (2912MF XL) • Two high-speed module slots accommodating 10/100, 100BASE-FX, Gigabit Ethernet (including 1000BASE-T), and GigaStack GBIC (2912MF XL and 2924M XL only) • Cisco switch clustering enabled • Managed	2-4
Catalyst 2950 Series	Fixed-configuration basic and Intelligent Ethernet 10/100 switches • 12/24/48 10/100 port managed switches with stackable and standalone models • Flexible uplink options: fixed 100Base FX, fixed 1000BaseT, fixed 1000BaseSX, and GBIC-based ports • Industrial-grade, rugged models (Catalyst 2955) for harsh environment deployments • Wire-speed, high performance switch • Models with the Standard Image software (SI) provide Layer 2 Cisco IOS functionality for basic data, voice, and video services at the edge of the network. • Models with the Enhanced Image software (EI) bring Layer 2-4 intelligent services such as advanced Quality of Service, rate limiting, security filtering and multicast management capabilities • Stackable up to 9 switches with Gigastack GBIC • Simplified network management through Cisco Cluster Management Suite up to 16 fixed configuration Catalyst switches	2-6
Catalyst 3500 Series XL	Fixed-configuration 10/100 and Gigabit Ethernet switches • 24 ports with 2 GBIC-based Gigabit Ethernet ports with in-line power(3524-PWR XL) • 8 GBIC-based ports (3508G XL) • Stackable up to 9 switches with GigaStack GBIC • Cisco Switch Clustering capable • Managed	2-10
Catalyst 3550 Series	Fixed-configuration Intelligent Ethernet switches in stackable 10/100, inline power, or Gigabit Ethernet configurations • Network control and bandwidth optimization via advanced Quality of Service (QoS), granular rate-limiting, Access Control Lists (ACLs), and multicast services • Network security through a wide range of authentication methods, data encryption technologies, and access restriction features based on users, ports, and MAC addresses • Network scalability through advanced routing protocols such as EIGRP, OSPF, BGP, and PIM (requires Enhanced Multilayer Software Image (EMI)) • Intelligent adaptability through Cisco Identity Based Networking Services (IBNS) offering greater flexibility and mobility to stratified users	2-12

Product	Features	Page
Catalyst 4500 Series-Modular Configuration (4503, 4506 and 4507R)	Modular, multilayer switch with integrated intelligent services for converged networks in enterprise campus wiring closets, Layer2/Layer3 distribution, and integrated LAN/WAN branch office. • Resilient architecture for mission critical applications • Up to 240 ports of Ethernet, Fast Ethernet or Gigabit Ethernet over Fiber or Copper • High performance, Cisco Express Forwarding (CEF) Layer 2/3/4 switching up to 48 Mpps • Up to 64 Gbps of switching capacity • Advanced network control with predictable performance, granular QoS, advanced security, comprehensive management • Managed	2-15
Catalyst 4000 Series—Fixed Configuration (4908G-L3 and 4912G)	High performance fixed Gigabit Ethernet switch with intelligent enterprise Cisco IOS services	2-17
Catalyst 5000 Family	Modular switch that supports a broad range of interfaces for aggregation of legacy technologies with IP technology • End of Sale Effective June 2003/End of Support effective 2008. For further information please contact your local sales representative	2-18
Catalyst 6500 Family	High-performance, multilayer switch with integrated intelligent services for enterprise campus backbones, server aggregation, or internet data centers • 10/100, 100FX Fast Ethernet, 1000BASE-T, 1000BASE-X, and Gigabit Ethernet modules • Layer 4-7 services • Up to 256 Gbps of switching capacity • Packet throughput scalable to 100+ Mpps • Managed	2-20
Catalyst 8500 Series	High-performance, modular, multimedia switch router • Wire speed, nonblocking IP, IPX, IP multicast Layer 3 switching • Multiple interface options • Managed	2-24

Cisco LAN and MAN Products Port Matrix

	Switches							
	Catalyst 2900	Catalyst 2900 XL	Catalyst 2950	Catalyst 3500 XL	Catalyst 3550	Catalyst 4500	Catalyst 6000	Catalyst 8500
Fixed Ports Only	X							
Fixed and Modular Ports		X	X	X	X	X		
Modular Ports Only							X	X
Ports								
10BASE-T Switched	X	X	X	X	X	X	X	
10BASE-FL Switched							X	
100BASE-T Switched	X	X	X	X	X	X	X	
100BASE-F Switched		X	X		X	X	X	X
10/100 Autosensing Switched	X	X	X	X	X	X	X	X
1000BASE-TX							X	
10/100/1000							X	
10GBASE-LR							X	
ATM							X	X
Gigabit Ethernet	X	X	X	X	X	X	X	X
Integrated In-Line Power				X		X	X	
Integrated Server Load Balancing							X	

Cisco Catalyst 2900 Series



The Catalyst 2948G and 2980G deliver all the Ethernet switching needed for many small to medium-sized wiring closets in a single system without the need for additional modules, cables or other interconnects. Utilizing the same industry-leading software and functionality of the Catalyst 4000, 5000, and 6000 families, the Catalyst 2948G and 2980G have consistent end-to-end services, which ensure complete interoperability with enterprise Catalyst switches.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 2980G Series	• A single box solution without additional cables, modules or configuration • Up to 80 ports of wire-speed, non-blocking performance with large MTBF reliability • End-to-end VLANs, EtherChannel, multicasting, and security • Mature/proven Catalyst software compatibility in the wiring closet and data center
Catalyst 2948G Series	• The same features as 2980G but up to 48 ports of wire-speed, non-blocking performance
Catalyst 2948G-L3	• High performance CPU with Cisco IOS software • Dedicated 48 ports of 10/100 Mbps and two ports of 1000BASEX Gigabit Ethernet with gigabit Ethernet converter (GBIC) support; all ports support Layer 3 capability

Key Features

- Powerful non-blocking performance with proven Cisco IOS services
- Wire speed 18 Million pps switching throughput
- Intelligent multilayer IOS services (security, multicast, quality of service [QoS])
- Advanced multiple queue QoS architecture
- Security (TACACS+, RADIUS, port lockdown)
- Spanning-Tree Protocol (802.1D) with enhancements (UplinkFast, PortFast) for deterministic/fast failover
- Redundant Power Supply (option)

Competitive Products

- HP Procurve: 4108gl, 4000M
- 3Com: SS3300
- Nortel/Bay: BayStack 350T and 450T
- Extreme: Summit 48si

Specifications

Feature	Catalyst 2980G	Catalyst 2948G-L3	Catalyst 2948G
Fixed Ports (connections)	80-port 10/100BASE-TX 2-port 1000BASE-X (GBIC)	48 port 10/100BASE-TX 2-port 1000BASE X (GBIC)	48-port 10/100BASE-TX 2-port 1000BASE-X (GBIC)
Backplane	24 Gbps	22 Gbps	24 Gbps
Stackable	No	No	No
Full-Duplex Capabilities	All ports	All ports	All ports
VLAN Maximum	1024	1024	1024
FEC	Yes	No	Yes
ISL	No	Yes	No
802.1Q	Yes	Yes	Yes
Management Capabilities	CiscoWorks 2000, CWSI, CiscoView, CDP, VTP, Enhanced SPAN, SNMP, Telnet Client, BOOTP, TFTP	CiscoWorks 2000, CWSI, CiscoView, CDP, VTP, Enhanced SPAN, SNMP, Telnet Client, BOOTP, TFTP	CiscoWorks 2000, CWSI, CiscoView, CDP, VTP, Enhanced SPAN, SNMP, Telnet Client, BOOTP, TFTP
Processor Speed (Type)	200 MHz (R5000 RISC)	200 MHz (R5000 RISC)	200 MHz (R5000 RISC)
Flash Memory	12 MB	16 MB	12 MB
DRAM Memory	64 MB	64 MB	64 MB

Feature	Catalyst 2980G	Catalyst 2948G-L3	Catalyst 2948G
Embedded RMON	Statistics, history, alarms, events	Statistics, history, alarm, events	Statistics, history, alarms, events
Dimensions (HxWxD)	3.5 x 17.5 x 17 in.	2.69 x 17.1 x 18 in.	2.62 x 17.5 x 15 in.
RPS	Yes (WS-C2980G-A), RPS 300	Yes, RPS 600	Yes, RPS 600

Selected Part Numbers and Ordering Information[1]

Catalyst 2900 Series Switches	
WS-2948G-L3	Catalyst 2948GL3 Switch
FR2948GL3-IP	Catalyst 2948G-L3 IP Switching License
FR2948GL3-IPX	Catalyst 2948G-L3 IPX Switching License
WS-C2948G	Catalyst 2948G Switch,48 10/100Tx (RJ-45) +2 1000x (GBIC Slots)
WS-C2948G-3PACK	3 Catalyst 2948G Switches
WS-C2980G-A	Catalyst 2980G Switch,80 10/100Tx (RJ-45) +2 1000x (GBIC Slots)
Catalyst 2900 Series Modules	
WS-G5484=	GBIC Module, fiber media SX
WS-G5486=	GBIC Module, fiber media LX/LH
WS-G5487=	GBIC Module, Fiber Media Zx
Mini-RMON Agent License	
WS-C2948G-EMS-LIC	Catalyst 2948G RMON Agent License
WS-C2980G-EMS-LIC	Catalyst 2980G RMON Agent Agreement
Catalyst 2900 Series Accessories	
WS-X2948G-RACK=	Catalyst 2948G Rack Kit (spare)
WS-X2980G-RACK=	Catalyst 2980G Rack Kit (Spare)
PWR600-AC-RPS-CAB=	Redundant Power Supply (RPS), 600 Watts (2948G only)
PWR600-AC-RPS-NCAB=	RPS 600 without Cable (2948G only)
PWR300-AC-RPS-N1=	RPS 300 with one Cable (2980G-A only)
CAB-RPS-1414=	One DC power cable for RPS 300
Catalyst 2900 Series Basic Maintenance	
CON-SNT-PKG8	Catalyst 2948G, 2948G-L3, and 2980G Packaged SMARTnet Maintenance 8x5xNBD

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 2900 Web site: **http://www.cisco.com/go/2900**

Cisco Catalyst 2900 Series XL—Modular Switches

Cisco's Catalyst 2900 Series XL is a full line of modular, 10/100 autosensing Fast Ethernet switches that combine outstanding performance, ease of use, and integrated Cisco IOS software.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 2912MF XL	• All-fiber switch to aggregate Fast Ethernet workgroups over 100BASE-FX connections in small and mid-size campus environments • High-speed uplinks to backbone or server via Fast Ethernet, Gigabit Ethernet
Catalyst 2924M XL	• Any combination of dedicated 10-Mbps or 100-Mbps connections to individual PCs, servers, and other systems or connectivity between existing Ethernet and Fast Ethernet workgroups • The option to easily increase the switch's port density and provide inexpensive high-speed uplinks through bandwidth aggregation (Fast EtherChannel and Gigabit EtherChannel technologies) • Gigabit Ethernet (including 1000BASE-T) modules for high-speed links • Hot swap insertion and removal of modules • Maximum flexibility

Key Features

- Switch fabric of 3.2 Gbps, a forwarding rate of more than 3.0 million packets per second, and a maximum forwarding bandwidth of 1.6 Gbps, delivering wire-speed performance across all 10/100 ports
- Support for IEEE 802.1p protocol for prioritization of mission-critical and time-sensitive applications such as voice and telephony traffic
- Cisco's switch clustering technology enables up to 16 interconnected Catalyst 1900, 2900 XL, and 3500 XL switches, regardless of geographic location, to form a flexible, single IP managed network
- Up to 250 port-based VLANs or ISL/802.1Q trunks
- Network port allows operation in networks with unlimited MAC addresses
- Autoconfiguration of multiple switches on a network from one boot server
- Up to 4 Gbps bandwidth between routers, switches, and servers with Fast EtherChannel and Gigabit EtherChannel technologies

Competitive Products

- 3Com: SuperStack III 3300
- Nortel: BayStack 350 & 450 switches

Specifications

Feature	Catalyst 2912 MF XL	Catalyst 2924M XL
Fixed Ports	12-port 100BASE-FX	24-port 10/100 autosensing
Modular Slots	2	Same as Catalyst 2912MF XL
Available Modules	4-port 10BASE-T/100BASE-TX autosensing 2-port or 4-port switched 100BASE-FX 1-port Gigabit Ethernet (1000BASE-T or GBIC-based)	Same as Catalyst 2912MF XL
Backplane	3.2 Gbps	Same as Catalyst 2912MF XL
Stackable	Yes	Same as Catalyst 2912MF XL
Full Duplex Capabilities	All 10BASE-T, 100BASE-TX, 100BASE-FX, 1000BASE-X, and 1000BASE-T	Same as Catalyst 2912MF XL
VLAN Maximum	250-port-based VLANs or ISL/802.1Q trunks	Same as Catalyst 2912MF XL
FEC	Yes	Same as Catalyst 2912MF XL
Inter-Switched Link	Yes	Same as Catalyst 2912MF XL
Flash Memory	4 MB	Same as Catalyst 2912MF XL
CPU DRAM	8 MB	Same as Catalyst 2912MF XL
Embedded RMON	History, Events, Alarms, Statistics	Same as Catalyst 2912MF XL
Dimensions (HxWxD)	3.46 x 17.5 x 12 in. (8.8 x 44.5 x 30.5 cm)	3Same as Catalyst 2912MF XL
Weight	13.5 lb (6.12 kg); 15 lb (6.8 kg) with two modules installed	Same as Catalyst 2912MF XL

Selected Part Numbers and Ordering Information[1]

Catalyst 2900 Series XL Switches	
WS-C2912MF-XL	12-port 100BASE-FX, 2 module slots
WS-C2924M-XL-EN	24-port 10/100 (autosensing), 2 module slots
WS-C2924M-XL-EN-DC	24-port 10/100 (autosensing), 2 module slots, DC powered
Catalyst 2900 Series XL Switch Bundles	
WS-C2924M-XL-EN-5P	Five Catalyst 2924M XL Switches
Catalyst 2900 Series XL Modules	
WS-X2914-XL-V	4-port 10/100 ISL/802.1Q Module
WS-X2924-XL-V	4-port 100BASE-FX ISL/802.1Q Module
WS-X2922-XL-V	2-port 100BASE-FX ISL/802.1Q Module
WS-X2931-XL	1-port, GBIC-based, 1000BASE-X Switch Uplink Module
WS-X2932-XL	1-port 1000BASE-T Switch Uplink Module
WS-X3500-XL	GigaStack GBIC
WS-G5484=	SX GBIC; 1000BASE-SX short wavelength, multimode fiber
WS-G5486=	LX GBIC; 1000BASE-LX/LH, long wavelength/long haul, single or multimode fiber
Catalyst 2900 Series XL Accessories	
CAB-GS-1M	1 meter cable for GigaStack GBIC
CAB-GS-50CM	50 centimeter cable for GigaStack GBIC

Catalyst 2900 Series XL Packaged SMARTnet Maintenance 8x5xNBD

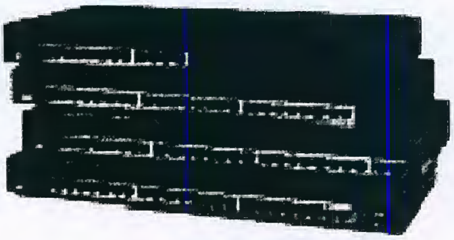
CON-SNT-PKG4	Catalyst 2900 Series WSC2924M-XL-EN Packaged SMARTnet 8x5xNBD
CON-SNT-PKG5	Catalyst 2900 Series WSC2924M-XL-EN-DC Packaged SMARTnet 8x5xNBD
CON-SNT-PKG7	Catalyst 2900 Series WSC2912MF-XL Packaged SMARTnet 8x5xNBD

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 2900 Series XL Web site: **http://www.cisco.com/go/2900xl**

Cisco Catalyst 2950 Series Intelligent Ethernet Switches



The Catalyst 2950 Series with Intelligent Ethernet Switches are fixed-configuration, standalone and stackable models that provide wire-speed Fast Ethernet and Gigabit Ethernet connectivity for small, mid-sized, service provider and industrial networks. The 2950C-24, 2950T-24, 2950G-12-EI, 2950G-24-EI, 2950G-48-EI and 2950G-24-EI-DC are part of an affordable product line that brings intelligent services, such as advanced quality of service, rate-limiting, security filters, and multicast management, to the network edge-while maintaining the simplicity of traditional LAN switching. When a Catalyst 2950 Switch is combined with a Catalyst 3550 Series Switch, the solution is capable of enabling IP routing from the edge to the core of the network. These Intelligent Ethernet Switches come with Enhanced Image (EI) software configuration only.

In addition to the range of Intelligent Ethernet switches, the Catalyst 2950 Series also includes switches with Standard Image (SI) software configuration only. The Cisco Catalyst 2950SX-24, 2950-24 and 2950-12, members of the Cisco Catalyst 2950 Series Switches, are standalone, fixed-configuration, managed 10/100 switches with Gigabit uplinks (2950SX-24 only) providing user connectivity for small to mid-sized networks. These wire-speed desktop switches come with Standard Image (SI) software features and offer Cisco IOS functionality for basic data, video and voice services at the edge of the network.

The Catalyst 2950 Series also includes the Cisco Catalyst 2955T-12, 2955C-12, and 2955S-12. The Cisco Catalyst 2955 are industrial-grade switches that provide Fast Ethernet and Gigabit Ethernet connectivity for deployment in harsh environments. With a range of copper and fiber uplink options, the Catalyst 2955 operates in environments such as industrial networking solutions (industrial Ethernet deployments), intelligent transportation systems (ITSs), and transportation network solutions. It is also suitable for many military and utility market applications where the environmental conditions or suspended solid concentrations exceed the specifications of other commercial switching products.

Embedded in all the products in the Catalyst 2950 Series is the Cisco Cluster Management Suite (CMS) Software, which allows users to simultaneously configure and troubleshoot multiple Catalyst desktop switches using a standard Web browser.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 2950 Series Intelligent Ethernet Switches with Enhanced Image (EI)	• Layer 2/3/4 based services: Advanced QoS, Security, High availability and STP enhancements • Wire-speed performance • Advanced QoS, Security, High availability and STP enhancements • Cisco Cluster Management • Stackable • GBIC based uplink ports for media flexibility
Catalyst 2950G-48-EI	• Ideal for desktop connectivity • High Port Density
Catalyst 2950G-24-EI	• Ideal for desktop connectivity • Medium Port Density
Catalyst 2950G-24-EI-DC	• Ideal for Telco/DCN environments • NEBS compliant • Medium Port Density
Catalyst 2950G-12-EI	• Ideal for desktop connectivity • Low Port density
Catalyst 2950T-24	• High speed uplink flexibility with fixed 10/100/1000BaseT ports • Low price per port
Catalyst 2950C-24	• High speed uplink flexibility over extended distances with fixed 100BASE-FX connections using MT-RJ connectors • Low price per port
Catalyst 2950 Series with Standard Image (SI)	• Wire speed, high performance switches for delivering 10/100 Mbps speed connectivity to desktop PCs, servers and other systems • Layer 2-based QoS and Security features • Cisco Cluster Management • Ideal for desktop connectivity,
Catalyst 2950-12	• Low Port density
Catalyst 2950-24	• Medium port density
Catalyst 2950SX-24	• High speed uplinks with 2 fixed 1000BaseSX ports • Medium port density
Catalyst 2955 Series with Enhanced Image (EI)	• Ideal for harsh network environments • Rugged: Implements industrial-grade components, a compact form factor, convection cooling, and relay output signaling. Designed to operate at extreme temperatures and under extreme vibration and shock. • Layer 2/3/4 based services: Advanced QoS, Security, High availability and STP enhancements • Wire-speed performance
Catalyst 2955T-12	• Twelve 10/100 ports and two 10/100/1000BASE-TX (Copper) uplinks
Catalyst 2955C-12	• Twelve 10/100 ports and two 100BASE-FX (Multimode Fiber) uplinks
Catalyst 2955S-12	• Twelve 10/100 ports and two 100BASE-LX (Singlemode Fiber) uplinks

Key Features

- Cisco Cluster Management (CMS) Software offers superior manageability, ease-of-use and ease-of-deployment and enhanced configuration wizards
- Wire-speed performance in connecting end-stations to the LAN
- Catalyst 2950: Ideal for small- and mid-sized networks
- Catalyst 2955: Ideal for harsh network environments
- Sophisticated Multicast Management via IGMP Snooping
- Scalability and high availability features
- Support for Cisco Redundant Power System 300 (RPS 300)
- Switches with Standard Image (SI) include these additional features:
  - Catalyst 2950SX-24 switch provides a cost-effective solution for Gigabit speeds over fiber, offering 2 1000BaseSX uplinks
  - QoS and Security based on Layer 2 information
  - Basic Cisco IOS Services

- Intelligent Ethernet Switches with Enhanced Image (EI) include these additional features:
  - Catalyst 2950T-24 switch is a component of the Cisco Gigabit Ethernet over copper solution, offering 10/100/1000BaseT uplinks
  - Powerful Gigabit-uplink options—GBIC-based or 1000BaseT
  - Superior control through advanced intelligent services—advanced quality of service based on Layer 2 through Layer 4 parameters
  - Superior Security features: based on Layer 2 through Layer 4 Access Control Parameters
  - Enhanced Cisco IOS Services

Competitive Products

- Hewlett Packard: Procurve 2500 /2650
- Nortel: BPS 2000/450T/420T
- 3 Com: Superstack 3300/4300/4400/4400SE/4200 series
- Extreme: Summit 24 e2e3
- Dell: Powerconnect 3024/3048/3248
- Hirshchmann
- GarretCom
- Sixnet

Specifications

Feature	Catalyst 2950G-48-EI	Catalyst 2950G-24-EI	Catalyst 2950G-24-EI-DC	Catalyst 2950G-12-EI	Catalyst 2950T-24
Fixed Ports	48 port 10/100 autosensing & 2 GBIC-based Gigabit Ethernet ports	24 port 10/100 autosensing & 2 GBIC ports	24 port 10/100 autosensing & 2 GBIC ports and DC Power	12 port 10/100 autosensing & 2 GBIC ports	26-port (24 10/100 autosensing & 2 ports 1000BaseT
Forwarding Bandwidth	13.6 Gbps	8.8 Gbps	8.8Gbps	6.4Gbps	8.8 Gbps
Forwarding Rate	10.1 Mpps	6.6 Mpps	6.6 Mpps	4.8 Mpps	6.6 Mpps
Full-Duplex Capabilities	All Ports	All Ports	All Ports	All Ports	All Ports
VLAN Maximum	250-port-based VLANS	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
FEC	Yes	Yes	Yes	Yes	Yes
802.1Q	Yes	Yes	Yes	Yes	Yes
Security	Port Security, with MAC aging, Private VLAN Edge, ACL, 802.11x, IBNS, SSH, RADIUS, TACACS+, SNMPv3 (crypto)	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
Multicast	IGMP Snooping	IGMP Snooping	IGMP Snooping	IGMP Snooping	IGMP Snooping
QoS	802.1P, 4 egress queues, WRR, SPS, Expedite Queuing, Policing, Marking, Layer 3 and 4 Services, Auto QoS	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
Management Capabilities	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
Software Image	Enhanced Image (EI)	Enhanced Image (EI)	Enhanced Image (EI)	Enhanced Image (EI)	Enhanced Image (EI)
Flash Memory	8 MB	8 MB	8 MB	8 MB	8 MB
CPU DRAM	16 MB	16 MB	16 MB	16 MB	16 MB
Embedded RMON	History, Events, Alarms, Statistics	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI	Same as Catalyst 2950G-48-EI
Dimensions (H x W x D)	1.72 x 17.5 x 13 in.	1.72 x 17.5 x 9.52 in.	1.72 x 17.5 x 9.52 in.	1.72 x 17.5 x 9.52 in.	1.75 x 17.5 x 16 in.

Feature	Catalyst 2950C-24	Catalyst 2950-24	Catalyst 2950-12	Catalyst 2950SX-24	Catalyst 2955 (T-12,C-12,S-12)
Fixed Ports	26-port (24 10/100 autosensing & 2 ports100BaseFX)	24-port 10/100 autosensing	12-port 10/100 autosensing	26-port (24 10/100 autosensing & 2 ports1000BaseSX)	12 10/100 ports T-12: 2 fixed 10/100/1000BASE-T uplink ports C-12:2 fixed 100BASE-FX multimode uplink ports S-12: 2 fixed 100BASE-LX single-mode uplink ports
Forward Bandwidth	5.2 Gbps	4.8 Gbps	2.4 Gbps	8.8 Gbps	13.6 Gbps
Forwarding Rate	3.9 Mpps	3.6 Mpps	1.8 Mpps	6.6 Mpps	2 Mpps
Full-Duplex Capabilities	All Ports	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	All Ports
VLAN Maximum	250-port-based VLANS	64-port-based VLANS	64-port-based VLANS	64-port-based VLANS	250-port-based VLANS
FEC	Yes	Yes	Yes	Yes	Yes
802.1Q	Yes	Yes	Yes	Yes	Yes
Security	Port Security, with MAC aging, Private VLAN Edge, ACL, 802.11x, IBNS, SSH, RADIUS, TACACS+, SNMPv3 (crypto)	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	Port Security, with MAC aging, Private VLAN Edge, 802.11x, RADIUS, TACACS+, SNMPv3 (non-crypto)
Multicast	IGMP Snooping	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24
QoS	802.1P, 4 egress queues, WRR, SPS, Expedite Queuing, Policing, Marking, Layer 3 and 4 Services, Auto QoS	802.1P, 4 egress queues, WRR	802.1P, 4 egress queues, WRR	802.1P, 4 egress queues, WRR	802.1P, 4 egress queues, WRR
Management Capabilities	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS	Same as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded CMS
Software Image	Enhanced Image (EI)	Standard Image (SI)	Standard Image (SI)	Standard Image (SI)	Enhanced Image (EI)
Flash Memory	8 MB	8 MB	8 MB	8 MB	16 MB
CPU DRAM	16 MB	16 MB	16 MB	16 MB	32 MB
Embedded RMON	History, Events, Alarms, Statistics	HSame as 2950 C-24	Same as 2950 C-24	Same as 2950 C-24	History, Events, Alarms, Statistics
Dimensions (H x W x D)	1.75 x 17.5 x 11.8 in.	1.75 x 17.5 x 11.8 in.	1.75 x 17.5 x 9.52 in.	1.75 x 17.5 x 9.52 in.	3.78x8.07x5.03in; connectors facing forward OR 5.03x8.07x3.78in; connectors facing downward

1730
3

Selected Part Numbers and Ordering Information[1]

Catalyst 2950 Series Switches

WS-C2950G-48-EI	Catalyst 2950G-48 switch with 48 10/100 ports and 2 Gigabit Interface Converter (GBIC)-based GE ports
WS-C2950G-24-EI	Catalyst 2950G-24 switch with 24 10/100 ports and 2 GBIC ports
WS-C2950G-24-EI-DC	Catalyst 2950G-24-DC switch with 24 10/100 ports, 2 GBIC ports and DC Power
WS-C2950G-12-EI	Catalyst 2950G-12 switch with 12 10/100 ports and 2 GBIC ports
WS-C2950T-24	Catalyst 2950C-24T switch with 24 10/100 ports and two fixed 1000BaseT Uplink ports
WS-C2950C-24	Catalyst 2950C-24 switch with 24 10/100 ports and two fixed 100BaseFX Uplink ports
WS-C2950-24	Catalyst 2950-24 switch with 24 10/100 ports
WS-C2950-12	Catalyst 2950-12 switch with 12 10/100 ports
WS-C2950SX-24	Catalyst 2950SX-24 switch with 24 10/00 ports and two fixed 1000BaseSX Uplink ports

Gigabit Interface Converters (GBICs)

WS-X3500-XL	GigaStack GBIC Gigabit Ethernet stacking GBIC and 50 cm cable
WS-G5484=	1000BaseSX GBIC short wavelength GBIC (multimode fiber only)
WS-G5486=	1000BaseLX/LH GBIC long wavelength/long haul GBIC (single or multimode fiber)
WS-G5487=	1000BaseZX GBIC extended-reach GBIC (single mode fiber only)
WS-G5483=	1000BaseT GBIC- Gigabit-Ethernet-over-copper GBIC

Redundant Power System (RPS)	
PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable
VAB-RPS-1414=	1.2 meter cable for Cisco RPS 300 to external device connection
Cables/Accessories	
CAB-RPS-1614=	1 RPS 675 connector cable 16/14
CAB-GS-50CM	50 centimeter cable for GigaStack GBIC
STK-RACKMOUNT-1RU=	Rack mount kit for 1 RU versions of Catalyst 2950, 3500 XL, 2900 XL, 1900, and FastHub 400 switches
Packaged SMARTnet 8x5xNBD Maintenance Contract	
CON-SNT-PKG3	Packaged SMARTnet 8x5xNBD Maintenance for the Catalyst 2950G-12, 2950-24 and 2950-12
CON-SNT-PKG4	Packaged SMARTnet 8x5xNBD Maintenance for the Catalyst 2950G-24 and 2850G-24-DC
CON-SNT-PKG6	Packaged SMARTnet 8x5xNBD Maintenance for the Catalyst 2950G-48

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 2950 Series Web site: **http://www.cisco.com/go/catalyst2950**

Cisco Catalyst 3500 Series XL

The Cisco Systems Catalyst 3500 series XL is a scalable line of stackable 10/100 and Gigabit Ethernet switches that delivers premium performance, flexibility, and manageability with unparalleled investment protection. This line of low-cost, high-performance switching solutions provides next-generation stackable switching through an independent high-speed stacking bus that preserves valuable desktop ports. Cisco's breakthrough Switch Clustering technology expands the stacking domain beyond a single wiring closet, enabling up to 16 interconnected Catalyst 3550, 2950, 3500 XL, 2950, 2900 XL and 1900 switches—regardless of geographic location—to form a flexible, single IP managed network.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 3524-PWR XL	• A stackable, wire-speed 10/100 and Gigabit Ethernet switch for delivering dedicated 10 or 100 Mbps to individual users and servers • Advanced QoS, high availability, and integrated in-line power enabling easy deployment of IP phones and wireless access points.
Catalyst 3508G XL	• A stackable Gigabit Ethernet switch with eight GBIC-based ports for aggregating a group of Gigabit Ethernet switches and servers through Cisco GigaStack GBICs or standard 1000BASE-X GBICs • Dedicated, high-speed Gigabit Ethernet performance

Key Features

- 10.8 Gbps switch fabric, up to 8 Mpps forwarding rate, and maximum forwarding bandwidth of 5.4 Gbps across all 10/100 ports
- Built-in Gigabit Ethernet ports accommodate a range of GBIC transceivers, including the Cisco GigaStack GBIC, 1000BASE-T, 1000BASE-SX and 1000BASE-LX/LH GBICs, and 1000BASE-ZX extended reach GBIC
- Low-cost, 2-port Cisco GigaStack GBIC offers a range of configurable stacking and performance options by delivering 1-Gbps connectivity in a daisy-chained connection or up to 2-Gbps in a dedicated, switch-to-switch connection
- Support for IEEE 802.1p technology for prioritization of mission-critical and time-sensitive application such as voice and telephony traffic
- 3524-PWR XL provides in-line power to IP phones and other devices

Competitive Products

- 3Com: SuperStack 3 Switch 3300 and 3900
- Hewlett Packard: ProCurve 2524, 2424M, 4000, and 8000
- Nortel: BayStack 450T and BPS 2000 switches

Specifications

Feature	Catalyst 3524-PWR XL	Catalyst 3508G XL
Fixed Ports	24-port 10/100 autosensing 2-port 1000BASE-X (GBIC)	8-port 1000BASE-X (GBIC)
Modular Slots	None	None
Backplane	10 Gbps	10 Gbps
Stackable	Yes	Yes
Full-Duplex	All ports	All ports
VLAN Maximum	250 port-based VLANs or ISL/802.1Q trucks	250 port-based VLANs or ISL/802.1Q trucks
FEC	Yes	Yes
Inter-Switch Link	Yes	Yes
In-Line Power	Yes	No
Management Capabilities	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded Cisco Visual Switch Manager, Web-based interface	SNMP, Telnet, RMON, CWSI, (CLI)-based out-of-band, embedded Cisco Visual Switch Manager, Web-based interface
Processors	Cisco designed ASICs	Cisco designed ASICs
Flash Memory	4 MB	4 MB
CPU DRAM	8 MB	8 MB
Embedded RMON	History, Events, Alarms, Statistics	History, Events, Alams, Statistics
Dimensions (HxWxD)	1.75 x 17.5 x 11.8 in	1.75 x 17.5 x 11.8 in

Selected Part Numbers and Ordering Information[1]

Catalyst 3500 Series XL Switches	
WS-C3524-PWR-XL-EN	24-port 10/100 (autosensing), 2 1000X GBIC Slots, inline power
WS-C3508G-XL-EN	8 1000X GBIC Slots
Catalyst 3500 Series XL Accessories	
WS-X3500-XL	GigaStack GBIC
WS-G5484=	1000BASE-SX GBIC
WS-G5486=	1000BASE- LX/LH GBIC
WS-G5487=	1000BASE- ZX extended reach GBIC
WS-G5483=	1000BASE-T GBIC
Catalyst 3500 Series XL Basic Maintenance	
CON-SNT-PKG4	Catalyst 3512 XL SMARTnet 8x5xNBD Maintenance
CON-SNT-PKG5	Catalyst 3524 XL and 3524-PWR XL SMARTnet 8x5xNBD Maintenance
CON-SNT-PKG6	Catalyst 3548 XL SMARTnet 8x5xNBD Maintenance
CON-SNT-PKG9	Catalyst 3508G XL SMARTnet 8x5xNBD Maintenance

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 3500 series XL Web site: **http://www.cisco.com/go/3500xl**

Cisco Catalyst 3550 Series Intelligent Ethernet Switches

The Cisco Catalyst 3550 Series Intelligent Ethernet Switches is a line of enterprise-class, stackable, multilayer switches that provide high availability, scalability, security and control to enhance the operation of the network. With a range of Fast Ethernet and Gigabit Ethernet configurations, the Catalyst 3550 Series can serve as both a powerful access layer switch for medium enterprise wiring closets and as a backbone switch for small networks. Now customers can deploy network-wide intelligent services, such as advanced quality of service, rate-limiting, Cisco security access control lists, multicast management, and high-performance IP routing—while maintaining the traditional LAN switching.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 3550 Series	• Enterprise-class intelligent services such as ACLs, advanced QoS, and rate-limiting • Cisco Cluster Management
Catalyst 3550-48-EMI (Enhanced Multilayer Software Image)	• High performance advancedIP routing • High Port Density • Ideal as a powerful access layer switch for a medium enterprise wiring closet with routed uplinks
Catalyst 3550-48-SMI (Standard Multilayer Software Image)	• High Port Density • Ideal for a powerful access layer switch for a medium enterprise wiring closet • Basic IP routing
Catalyst 3550-24-EMI (Enhanced Multilayer Software Image)	• High performance advancedIP routing • Medium Port Density • Ideal for a powerful access layer switch for a medium enterprise wiring closet with routed uplinks
Catalyst 3550-24-SMI (Standard Multilayer Software Image)	• Medium Port Density • Ideal for a powerful access layer switch for a medium enterprise wiring closet • Basic IP routing
Catalyst 3550-24PWR-EMI (Enhanced Multilayer Software Image)	• High performance advancedIP routing • Medium Port Density • Integrated inlinepower to Cisco IP telephones and Cisco wireless LAN access points • Ideal for a powerful access layer switch for a medium enterprise wiring closet with routed uplinks
Catalyst 3550-24PWR-SMI (Standard Multilayer Software Image)	• Medium Port Density • Integrated inlinepower to Cisco IP telephones and Cisco wireless LAN access points • Ideal for a powerful access layer switch for a medium enterprise wiring closet • Basic IP routing
Catalyst 3550-24-DC-SMI (Standard Multilayer Software Image)	• Medium Port Density • DC powered, NEBS level 3 compliant • Basic IP routing
Catalyst 3550-24-FX-SMI (Standard Multilayer Software Image)	• Medium Port Density • Ideal for 100FX aggregation • Basic IP routing
Catalyst 3550-12G	• High performance IP routing • Gigabit Ethernet aggregation using fiber • Ideal for stack aggregation, server aggregation, or as a backbone switch in a mid-sized network
Catalyst 3550-12T	• High performance advancedIP routing • Gigabit Ethernet aggregation using Category 5 copper cabling • Ideal for stack aggregation, server aggregation, or as a backbone switch in a mid-sized network
CD-3550-EMI	• High performance advancedIP routing • EMI upgrade kit for standard versions of the Catalyst 3550-24, 3550-24 PWR, 3550-24-DC, 3550-24-FX, and 3550-48 switches

Key Features

- Network control and bandwidth optimization via advanced Quality of Service (QoS), granular rate-limiting, Access Control Lists (ACLs), and multicast services
- Network security through a wide range of authentication methods, data encryption technologies, and access restriction features based on users, ports, and MAC addresses
- Network scalability through advanced routing protocols such as EIGRP, OSPF, BGP, and PIM (requires Enhanced Multilayer Software Image (EMI))
- Intelligent adaptability through Cisco Identity Based Networking Services (IBNS) offering greater flexibility and mobility to stratified users
- Lower Total Cost of Ownership (TCO) for IP Telephony and Wireless LAN deployments through integrated inline power (Catalyst 3550-24 PWR only)
- Easy switch configuration and deployment of advanced services through the embedded Cluster Management Suite (CMS) Software
- Stackable up to 9 switches with the Gigastack GBIC

Competitive Products

- Extreme Networks: Summit5i, Summit 24/48, Summit 48i
- Foundry: FastIron 4802
- Nortel: BPS 2000

Specifications

Feature	Catalyst 3550-48	Catalyst 3550-24	Catalyst 3550-24PWR	Catalyst 3550-12G	Catalyst 3550-12T	Catalyst 3550-24-DC	Catalyst 3550-24-FX
Fixed Ports	48 10/100 ports 2 GBIC-based Gigabit Ethernet ports	24 10/100 ports 2 GBIC-based Gigabit Ethernet ports	24 10/100 ports 2 GBIC-based Gigabit Ethernet ports	10 GBIC-based Gigabit Ethernet ports 2 10/100/1000 ports	10 10/100/1000 ports 2 GBIC-based Gigabit Ethernet ports	24 10/100 ports2 GBIC-based Gigabit Ethernet port	24 100FX MMF ports 2 GBIC-based Gigabit Ethernet port
Switching Fabric	13.6 Gbps	8.8 Gbps	8.8 Gbps	24 Gbps	24 Gbps	8.8 Gbps	8.8 Gbps
VLAN Maximum	1005	1005	1005	1005	1005	1005	1005
FEC/GEC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GBICs	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX, CWDM	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX	Gigastack, 1000BaseT, SX, LX/LH, ZX
802.1Q and ISL	Yes	Yes	Yes	Yes	Yes	Yes	Yes
In-Line Power	No	No	No	No	No	No	No
QoS	802.1p, DSCP, 4 egress Queues, WRR, Strict Priority Queuing,WRED	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48
Multicast	IGMP Snooping, PIM (requires EMI), DVMRP (requires EMI), CGMP Server (requires EMI)	IGMP Snooping, PIM (requires EMI), DVMRP (requires EMI), CGMP Server (requires EMI)	IGMP Snooping, PIM (requiresEMI), DVMRP (requires EMI), CGMP Server (requires EMI)	IGMP Snooping, PIM, DVMRP, CGMP Server	IGMP Snooping, PIM, DVMRP, CGMP Server	IGMP Snooping, PIM (requires EMI), DVMRP (requires EMI), CGMP Server (requires EMI)	IGMP Snooping, PIM (requires EMI), DVMRP (requires EMI), CGMP Server (requires EMI)
Management Capabilities	SNMP, Telnet, RMON, CWSI, CLI-based out-of-band, embedded CMS	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48
Flash Memory	16 MB	16 MB	16 MB	16 MB	16 MB	16 MB	16 MB
CPU DRAM	64 MB	64 MB	64 MB	64 MB	64 MB	64 MB	64 MB

Feature	Catalyst 3550-48	Catalyst 3550-24	Catalyst 3550-24PWR	Catalyst 3550-12G	Catalyst 3550-12T	Catalyst 3550-24-DC	Catalyst 3550-24-FX
Embedded RMON	History, Events, Alarms, Statistics	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48	Same as Catalyst 3550-48
Dimensions (H x W x D)	1.75 x 17.5 x 16.3 in.	1.75 x 17.5 x 14.4 in.	1.75 x 17.5 x 17.4 in.	2.63 x 17.5 x 15.9 in.	2.63 x 17.5 x 15.9 in	1.75 x 17.5 x 14.4 in.	1.75 x 17.5 x 16.3 in.

Selected Part Numbers and Ordering Information[1]

Catalyst 3550 Series Intelligent Ethernet Switches

WS-C3550-48-SMI	Catalyst 3550-48 multilayer switch with 48 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; SMI installed
WS-C3550-48-EMI	Catalyst 3550-48 multilayer switch with 48 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; EMI installed
WS-C3550-24-SMI	Catalyst 3550-24 multilayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; SMI installed
WS-C3550-24-EMI	Catalyst 3550-24 multilayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; EMI installed
WS-C3550-24PWR-SMI	Catalyst 3550-24 multilayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; integrated inline power; SMI installed
WS-C3550-24PWR-EMI	Catalyst 3550-24 multilayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernet ports; integrated inline power; EMI installed
WS-C3550-24-DC-SMI	Catalyst 3550-24-DC multiplayer switch with 24 10/100 ports and 2 GBIC-based Gigabit Ethernetports; SMI installed; DC-powered
WS-C3550-24-FX-SMI	Catalyst 3550-24-FX multilayer switch with 24100FX multimode fiber ports and 2 GBIC-based Gigabit Ethernet ports; SMI installed
WS-C3550-12G	10 GBIC-based Gigabit Ethernet ports and 2 10/100/1000 ports; EMI installed
WS-C3550-12T	10-10/100/1000BaseT ports and 2 GBIC-based Gigabit Ethernet ports; EMI installed
CD-3550-EMI=	EMI upgrade kit for the standard versions of the Catalyst 3550-24, 3550-48, 3550-24PWR, 3550-24-DC, and 3550-24-FX

Gigabit Interface Converters (GBICs)

WS-X3500-XL	GigaStack Stacking GBIC and 50 cm cable
WS-G5484=	1000BaseSX GBIC-short wavelength GBIC (multimodefiber only)
WS-G5486=	1000BaseLX/LH GBIC-long wavelength/long haul GBC (single or multimode fiber)
WS-G5487=	1000BaseZX GBIC-extendedreach GBIC (singlemode fiberonly)
WS-G5483=	1000BaseT GBIC-Gigabit Ethernetover Copper GBIC

Redundant Power System (RPS)

PWR675-AC-RPS-N1=	675W Redundant Power Supply with 1 connector cable
VAB-RPS-1414=	1.2 meter cable for CiscoRPS 300 to externaldevice connection

Cables/Accessories and Redundant Power Supply

CAB-RPS-1614=	1 RPS 675 connectorcable 16/14
RCKMNT-3550-1.5RU=	Rack mount kit for the Catalyst 3550-12T and 3550-12G switches
RCKMNT-1RU=	Rack mount kit for the Catalyst 3550-24, 3550-48, 3550-24PWR, 3550-24-DC, and 3550-24-FX switches

Packaged SMARTnet 8x5xNBD Maintenance Contract for Two-Tier Customers

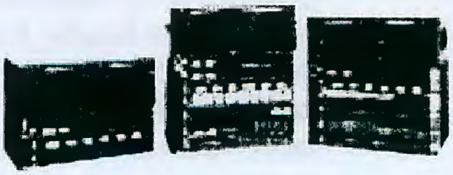
CON-SNT-PKG9	Packaged SMARTnet 8x5xNBD for the WS-C3550-12T and WS-C3550-12G
CON-SNT-PKG4	Packaged SMARTnet 8x5xNBD for the WS-C3550-24-SMI and WS-C3550-24PWR-SMI
CON-SNT-PKG5	Packaged SMARTnet 8x5xNBD for the WS-C3550-24-DC-SMI
CON-SNT-PKG6	Packaged SMARTnet 8x5xNBD for the WS-C3550-24-EMI, WS-C3550-24PWR-SMI and WS-C3550-48-SMI
CON-SNT-PKG7	Packaged SMARTnet 8x5xNBD for the WS-C3550-48-EMI and WS-C3550-24-FX-SMI

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 3550 Series Web site: **http://www.cisco.com/go/cat3550**

Cisco Catalyst 4500 Series



The Cisco Catalyst 4500 Series integrates nonblocking Layer 2/3/4 switching with optimal control, enabling business resilience for enterprise and metropolitan Ethernet customers deploying Internet-based business applications. A next generation Catalyst 4000 Series platform, the Cisco Catalyst 4500 Series includes three new chassis: Catalyst 4507R (7-slot: redundant Supervisor IV capable), Catalyst 4506 (6-slot) and Catalyst 4503 (3-slot). A key component of Cisco AVVID (Architecture for Voice, Video and Integrated Data), the Catalyst 4500 extends control to Enterprise wiring closets, branch office and Layer 3 distribution points. A variety of network infrastructure solutions are enabled by the Catalyst 4500 Series of switches including: Cisco IOS Network Services, IP Telephony, 10/100/1000 to the desktop, Wireless LAN, NetFlow Services and Metro Ethernet Switching.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 4507R	• When network resiliency via redundant Supervisor Engines is crucial to customer success • Port density up to 240-10/100, 100-FX, or 10/100/1000BASE-T with modular investment protection • Layer 2 and Layer 3 Cisco Express Forwarding (CEF)-based switching up to 64 Gbps, 48 Mpps
Catalyst 4506	• Port density up to 240-10/100, 100-FX, or 10/100/1000BASE-T with modular investment protection • Layer 2 and Layer 3 Cisco Express Forwarding (CEF)-based switching up to 64 Gbps, 48 Mpps
Catalyst 4503	• Port density up to 96-10/100, 100-FX, or 10/100/1000BASE-T with modular investment protection • Layer 2 and Layer 3 Cisco Express Forwarding (CEF)-based switching up to 28 Gbps, 21 Mpps

Note: Compatible sparing between Catalyst 4507R, 4506, and 4503 chassis provides investment protection with common power supplies and switching line cards. The Catalyst 4500 series also leverages the same feature set with identical software code base along with the same enterprise functionality as the Catalyst 6500 Series in the wiring closet, delivering a consistent end-to-end solution.

Key Features

- Supervisor II
  - Catalyst 4500/6500 Series CatOS Software, single IPQ—Address Management, and security (TACACS+, port lockdown, RADIUS, Kerberos)
  - Enterprise VLANs (4,096) with 802.1Q support on all ports, 16,000 MAC Addresses, and Spanning-Tree Protocol (802.1D) enhancements (UplinkFast, PortFast, and BackboneFast) for deterministic/fast failover
  - Fast and Gigabit EtherChannel aggregation (up to 8 Gbps full duplex), load balancing and failover on every port, and port filtering
- Supervisor IV
  - Capable of 1+1 redundancy in a 4507R (Single Supervisor only in Catalyst 4506 and 4503)
  - Optional NetFlow Services Card Support
  - Integrated Layer 2/3/4 CEF based switching at 64Gbps and 48Mpps
  - Feature rich and proven Cisco IOS Software
  - Port based enhanced QOS with multiple queues (16k input; 16k output), bandwidth management, policing and Access Control Lists (16k input ACL entries; 16k output entries)
  - Enterprise VLANs (4,000) with 802.1Q and ISL support on all ports, 32,000 MAC Addresses, and Spanning-Tree Protocol (802.1D), 802.3w, 802.3s

- Supports RIP I, RIP II, Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP) Enhanced IGRP (EIGRP), BGP4, IS:IS, Software based IPX and Appletalk, Hot Standby Router Protocol (HSRP), Cisco Group Management Protocol (CGMP), IGMP v1 and II, Internet Control Message Protocol (ICMP), and both Protocol Independent Multicast (PIM) sparse and dense modes, and Distance Vector Multicast Routing Protocol (DVMRP) interoperability
- Optional compact flash memory cards

7723 ε

Competitive Products

- Extreme Networks: Alpine 3802, Alpine 3804, and Alpine 3808
- Enterasys: Matrix E-5, Matrix E-6, Matrix E-7
- Foundry: FastIron 400/800, FastIron II, II+, III, BigIron4000
- Hewlett Packard: Procurve 5300XL, 4108GL
- Nortel: Passport 8100

Specifications

Feature	Catalyst 4507R	Catalyst 4506	Catalyst 4503
Fixed Ports	2 Gigabit uplink ports on Supervisor IV	2 Gigabit uplink ports on Supervisor Engine II, III and Supervisor IV	2 Gigabit uplinkports on Supervisor Engine II, IIIand Supervisor IV
Maximum Port Density	240 (10/100 Fast Ethernet) 240 (100-FX Fast Ethernet) 240 (10/100/1000BASE-T)	240 (10/100 Fast Ethernet) 240 (100-FX Fast Ethernet) 240 (10/100/1000BASE-T)	96 (10/100 Fast Ethernet) 96 (100-FX Fast Ethernet) 96 (10/100/1000BASE-T)
Modular Slots	7 (2 for Supervisors	6 (1 for Supervisor)	3 (1 for Supervisor)
Available Modules	Supervisor Engine IV	Supervisor Engine II, III, and IV	Supervisor Engine II, III, and IV
Redundant Supervisor Capable	Yes	No	No
Backplane Capacity	64 Gbps	64 Gbps	28 Gbps
Stackable	No	No	No
Hot-Swappable Power Supplies	Yes (2 bays, 1+1)	Yes (2 bays, 1+1)	Yes (2 bays, 1+1)
Embedded RMON	Statistics, History, Alarm, Events	Statistics, History, Alarm, Events	Statistics, History, Alarm, Events
Dimensions (H x W x D)	19.19 x 17.31 x 12.50 in 48.74 x 43.97 x 31.70 cm	17.38 x 17.31 x 12.50 in 44.13 x 43.97 x 31.70 cm	12.25 x 17.31 x 12.50 in 31.12 x 43.97 x 31.70 cm

Selected Part Numbers and Ordering Information[1]

Catalyst 4500 Series Switches	
WS-C4507R	Catalyst 4500 Chassis (7-Slot),fan, no p/s, Red Sup Capable
WS-C4506	Catalyst 4500 Chassis (6-Slot),fan, no p/s
WS-C4503	Catalyst 4500 Chassis (3-Slot),fan, no p/s
Catalyst 4500 Series Common Equipment	
WS-X4013=	Catalyst 4000 Supervisor Engine II, Console(RJ-45), Mgt. (RJ-45) (Spare)
WS-X4014=	Catalyst 4000 Supervisor III (2 GE), Console(RJ45)
WS-X4515=	Catalyst 4000 Supervisor IV, 2 GE, Console(RJ-45)
WS-F4531=	Catalyst 4000 NetFlow Services card for Supervisor Engine IV
PWR-C45-1000AC=	Catalyst 4500 1000W AC Power Supply(Data Only)
PWR-C45-1300ACV=	Catalyst 4500 1300W AC Power Supplywith Int Voice
PWR-C45-2800ACV=	Catalyst 4500 2800W AC Power Supplywith Int Voice
Catalyst 4000 Series Common Equipment	
WS-C4003-S1	Catalyst 4003 Chassis (3-Slot), Supervisor Engine 1, 1-AC Power Supply, Fan Tray, Rack-Mount Kit
WS-C4006-S2	Catalyst 4006 Chassis (6-Slot), Supervisor II, (2)AC Power Supplies,Fan Tray, Rack-Mount Kit
WS-C4006-S3	Catalyst 4006 Chassis (6-slot), Supervisor III, (2) AC Power Supplies, Fan Tray, Rack-Mount Kit
WS-C4006-S4	Catalyst 4006 Chassis (6-slot), Supervisor IV, (2) AC Power Supplies, Fan Tray, Rack-Mount Kit
WS-X4008=	Catalyst 4003/4006 AC Power Supply (Spare)
WS-X4095-PEM=	Catalyst 4000 DC Power Entry Module (Spare)
WS-P4603-2PSU	Catalyst 4000 Aux. Power Shelf with 2 PSU
WS-X4608=	Catalyst 4603 Power Supply Unit for WS-P4603

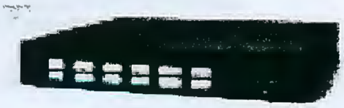
Catalyst 4500 Series Line Card Modules and GBICs	
WS-X4124-FX-MT=	Catalyst 4000 FE Switching Module, 24-port 100FX (MTRJ)
WS-X4148-FX-MT=	Catalyst 4000 FE Switching Module, 48-100FX MMF (MTRJ)
WS-X4148-RJ=	Catalyst 4000 10/100 Fast Ethernet Module, 48 Ports (RJ-45)
WS-X4148-RJ21=	Catalyst 4000 Telco switch module, 48-port 10/100 (4xRJ21)
WS-X4148-RJ45V=	Catalyst 4000 Inline Power 10/100, 48-port (RJ45)
WS-X4232-GB-RJ=	Catalyst 4000 E/FE/GE Module, 2-GE (GBIC), 32-10/100 FE (RJ-45)
WS-X4232-RJ-XX=	Catalyst 4000 FE Base Module, 32-10/100(RJ45)+ Modular Uplink slot
WS-X4232-L3=	Catalyst 4000 E/FE/GE L3 Module, 2-GE(GBIC), 32-10/100 (RJ45)
WS-X4306-GB=	Catalyst 4000 Gigabit Ethernet Module, 6 Ports (GBIC)
WS-X4424-GB-RJ-45=	Catalyst 4000 24 port 10/100/1000 Auto-Sensing Module (RJ45)
WS-X4448-GB-RJ45=	Catalyst 4000 48 port 10/100/1000 Auto-Sensing Module (RJ45)
WS-X4418-GB=	Catalyst 4000 GE Module, Server Switching 18 Ports (GBIC)
WS-U4504-FX-MT=	Catalyst 4000 FE Uplink Daughter Card, 4-port 100FX (MTRJ)
WS-X4604-GWY=	Catalyst 4000 Access Gateway Module with IP/FW software
WS-G5483=	1000BASE-T GBIC (RJ-45)
WS-G5484=	1000BASE-SX Shortwave GBIC Module (Multimode Only)
WS-G5486=	1000BASE-LX/LH Long Haul GBIC Module (Multimode or Single Mode)
WS-G5487=	1000 BASE-ZX GBIC module (Single Mode Only)
Catalyst 4500 Series Software	
S4KL3-12113EW=	Cisco IOS BASIC L3 SW Cat4500 SUP 3/4(RIP,St.Routes,IPX,AT)
S4KL3E-12113EW=	Cisco IOS ENHANCED L3 SW Cat4500 SUP3/4(OSPF,IGRP,EIGRP,IS-IS)
SC4K-SUPK8-7.5.1=	Catalyst OS L2 SW Cat4500 Sup 2
WS-C4006-EMS-LIC	Catalyst 4006 RMON Agent License
WS-C4003-EMS-LIC	Catalyst 4003 RMON Agent License
Catalyst 4500 Series Basic Maintenance	
CON-SNT-PKG11	Catalyst 4003 SMARTnet 8x5xNBD Maintenance
CON-SNT-PKG12	Catalyst 4006 SMARTnet 8x5xNBD Maintenance

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 4500 series Web site: **http://www.cisco.com/go/cat4000**

Cisco Catalyst 4000 Series — Fixed Configuration



Cisco offers two dedicated Gigabit Ethernet fixed configuration switches; the Catalyst 4908G-L3 and the Catalyst 4912G. The Catalyst 4908G-L3 Switch is a fixed configuration Layer 3 Ethernet switch featuring wire-speed switching for IP, IPX and IP Multicast. It provides the high performance required for midsize campus backbones with optimum port density.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 4908G	• Cost effective dedicated Gigabit Ethernet Layer 3 backbone solution ideal for deployment in midsize networks for those customers who need wire speed Layer 3 performance but do not require Gigabit Ethernet density over 8 ports.
Catalyst 4912G	• Advanced wirespeed, non-blocking Layer 2 Gigabit Ethernet performance wth intelligent Cisco IOS services and high-speed connections to workstations or servers; flexible Gigabit Interface Converter (GBIC) interfaces on all ports

Key Features

- Catalyst 4908G-L3:
  - 8 ports of 1000BASE x Gigabit Ethernet with GBIC support; Layer 3 switching and routing of IP, IPX and IP Multicast with wire speed Layer 2 switching for non routable protocols; Gigabit Etherchannel capability on every port
- Catalyst 4912G:
  - Wire-speed performance with 24 Gbps of dedicated bandwidth for nonblocking Gigabit Ethernet concentration, broad Gigabit EtherChannel availability, and GBIC flexibility on fiber port interfaces covering a wide range of cabling distances

Competitive Products

- Extreme Networks: Summit 1
- Foundry: Turbo Iron 8
- Nortel: Accellar 1200

Specifications

Feature	Catalyst 4908G-L3	Catalyst 4912G
Fixed Ports	8 (All Layer 3)	12 (All Layer 2)
Backplane Capacity	22 Gbps	24 Gbps
Stackable	No	No
VLAN Maximum	244	244
802.1Q	Yes	Yes
ISL	Yes	No
Management Capabilities	Inboard console via terminal or modem, outboard via Telnet, SNMP, CiscoView, CWSI, CiscoWorks 2000	Inboard console via terminal or modem, outboard via Telnet, SNMP, CiscoView, CWSI, CiscoWorks 2000
Dimensions (H x W x D)	2.69 x 17.1 x 18in	2.75 x 17.5 x 15 in.

Selected Part Numbers and Ordering Information[1]

Catalyst 4000 Switch Family	
WS-4908G-L3	Catalyst 4908G-L3 switch
WS-C4912G	Catalyst 4912G switch, fixed 12-ports switched 1000BASE-X (GBIC)
WS-G5484=	1000BASE-SX GBIC module
WS-G5486=	1000BASE-LX/LH GBIC module
WS-G5487=	1000BASE-ZX GBIC module

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 4000 series Web site: **http://www.cisco.com/go/cat4000**

Cisco Catalyst 5000 Family

On October 4, 2002, Cisco Systems announced the end of sale for the Cisco Catalyst 5000 and 5500 series of modular switches, including all related Cisco Catalyst 5000 and 5500 series chassis and modules. The Cisco Catalyst 5000 and 5500 series chassis and modules will be orderable through June 30, 2003.

The Catalyst 5000 family features a Gigabit Ethernet and ATM-ready platform offering users high-speed trunking technologies, including Fast EtherChannel and OC-12 ATM. This series also provides a redundant architecture, dynamic VLANs, complete intranet services support, and media-rate performance with a broad variety of interface modules.

Migration Options

	When a Customer Needs These Features
Catalyst 6500 with Sup2/msfc2	• High Performance L3 wiring closet, data centre,or core feature sets • Integrated L2-7 Serices Modules • Layer 3 Routing Capabilities • Scalability to 256 Gbps • Hardware based QoS and ACLs • IOS software
Catalyst 6500 with Sup2/pfc2	• High Performance L2 wiring closet, data centreor core feature sets • Scalability to 256 Gbps • Hardware based QoS and ACLs
Catalyst 6500 with sup1A-2GE	• Low cost of entry wiring closet solution • Scalability to 32Gbps • Basic security and L2 QoS capabilities • L2 Stateful failover capabilities

Competitive Products

- Enterasys: Matrix E7, Expedition ER16
- Nortel: Passport 8100, 8600
- Extreme: Black Diamond
- Foundry: Big Iron

Specifications

Feature	Catalyst 5500	Catalyst 5505	Catalyst 5509
Modular Slots	13	5	9
Available Modules	Supervisor[1] Engine II G, III G, or III plus any combination of modules (subset listed under Part Numbersand Ordering Information)	Same as Catalyst 5500	Same as Catalyst 5500
Backplane	3.6 Gbps ATM switching: 5-Gbps backplane	3.6 Gbps	3.6 Gbps
Full-Duplex Capabilities	All Ethernet, Fast Ethernet, Token Ring, and ATM ports	Same as Catalyst 5500	Same as Catalyst 5500
VLAN Maximum	Spanning tree: Yes per VLAN 1000 VLANs	Same as Catalyst 5500	Same as Catalyst 5500
FEC	100BASE-TX; 100BASE-FX; 1000 BASE-X	Same as Catalyst 5500	Same as Catalyst 5500
Management Capabilities	Inboard console via terminal or modem, outboard via Telnet, SNMP, CiscoView, CWSIStatistics, history, alarms, events	Same as Catalyst 5500	Same as Catalyst 5500
Dimensions (HxWxD)	25.25 x 17.3 x 18.25 in.	10.4 x 17.2 x 18.14 in.	20 x 17.25 x 18.14 in.

1. Supervisor module(s) require a slot in the chassis.

Selected Part Numbers and Ordering Information[1]

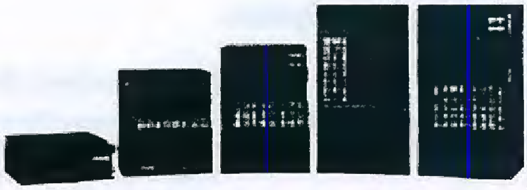
Catalyst 5000 Family Switch Families	
WS-C5507=	13-slot Chassis, AC Power Supply
WS-C5505-CHAC=	Catalyst 5505 Chassis, AC Power Supply
WS-C5509-CHAC=	Catalyst 5509 Spare Chassis, AC Power Supply
WS-C5509-CHDC=	Catalyst 5509 Spare Chassis, DC Power Supply
Catalyst 5000 Family Basic Maintenance	
CON-SNT-PKG13	Catalyst 5505 Packaged SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG16	Catalyst 5500 Packaged SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG15	Catalyst 5509 Packaged SMARTnet Maintenance 8x5xNBD

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Catalyst 5500/5000 series Web site: **http://www.cisco.com/go/5000**

Cisco Catalyst 6500 Family



The Catalyst 6500 Family delivers highly available secure converged network services for the Enterprise and Service Provider networks. Designed to address the increased requirements for gigabit scalability, high-availability, rich services, and multilayer switching in backbone, distribution, and wiring closet topologies as well as datacenter environments, the Catalyst 6500 Family delivers exceptional scalability and price/performance, supporting a wide range of interface densities, performance, and integration of powerful service modules. The Catalyst Family delivers a wide range of intelligent switching solutions, enabling corporate intranets, extranets, and the internet for multimedia, mission-critical data, and voice applications.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 6500 Series	• A highly scalable platformthat meets requirements for a dynamic environment includingvery high multilayer switching performancewith high Fast Ethernet and Gigabit Ethernetport densities
Catalyst 6500 Family Solutions	• Enterprise campus distribution and core—Withindustry-leading port densities, performance, and high availability solutions • Enterprise Server Farm—For Gigabit wire-speed access to mission-critical server farms • High-capacitywiring closets—In very large deployments, the Catalyst 6000 family delivers advanced Layer 2, 3, and 4 switching in wiring closets • Value wiring closets where basic L2 QoS and ACL capabilities are required in addition to 2-3 Sec L2 Stateful failover • WAN/LAN/MAN integration—Single integated platform simplifies network design, decreases rack space requirements, and decreases overall administration costs • Advanced, integrated hardwae based firewall, contentswitching, intrusion detection, and network analysis capabilies • Service Provider Networks—For all dynamic environments including e-commerce, web hosting, and co-location facilities

Key Features

- Application-aware networking with multilayer switching intelligence and support for CiscoAssure policy networking
- High-availability features deliver maximum uptime for mission-critical application support
- Extensive Quality of Service (QOS) features to support mission-critical applications
- Scalable performance to 210 Mpps
- Maximum 10/100 Ethernet port density: 96 (3-slot chassis), 240 (6-slot chassis), 384 (9-slot chassis), and 576 (13-slot chassis)
- Maximum Gigabit Ethernet port density: 32 (3-slot chassis), 82 (6-slot chassis), 130 (9-slot chassis), and 194 (13-slot chassis)

Competitive Products

- Extreme: Black Diamond
- Foundry: Big Iron
- Lucent: Cajun Switch 550
- Nortel: Passport 8600

Specifications

Feature	6503	6506	6509	6513
Modular Slots	3	6	9	13
Available Modules	8 & 16 port Gigabit Ethernet 24 port 100FX Ethernet (multimode or single mode); 48 port 10/100TX Ethernet (RJ45); 48 port 10/100 Ethernet (RJ 21 or TELCO); 1 port Multimode OC12 ATM; 1 port Single Mode OC 12 ATM; 15 port 1000BASE T Gigabit Ethernet; 24 port 10BASE FL (MT RJ); Network Analysis Module; Flex Wan Module; 24 port FXS Analog Station Interface Module; 8 port Voice T1 or E1 Services Module; Voice Power Feature CardIntrusion Detection Module; Content Switching Module; Fabric Enabled Line Cards	Same as Catalyst 6503	Same as Catalyst 6503	Same as Catalyst 6503 plus: Switch Fabric Module 2
Backplane	Scalable to 256 Gbps	Scalable to 256 Gbps	Scalable to 256 Gbps	Scalable to 256 Gbps
Multilayer Performance	Scalable to 100+ Mpps	Scalable to 100+ Mpps	Scalable to 100+ Mpps	Scalable to 210 Mpps
VLAN Maximum	4000	4000	4000	4000
FEC/GEC	Up to 8 noncontiguous ports; supports multimode channeling.	Same as Catalyst 6503	Same as Catalyst 6503	Same as Catalyst 6503
Management Capabilities	CiscoWorks 2000, RMON, Enhanced Switched Port Analyzer (ESPAN), SNMP, Telnet, BOOTP, and Trivial File Transfer Protocol (TFTP)	Same as Catalyst 6503	Same as Catalyst 6503	Same as Catalyst 6503
Dimensions	7 x 17.37 x 21.75 in.	20.1 x 17.2 x 18.1 in.	25.2 x 17.2 x 18.1 in.	33.3 x 17.2 x 18.1 in.

Selected Part Numbers and Ordering Information[1]

Catalyst 6000 Family Chassis	
WS-C6503	Catalyst 6500 3 Slot Chassis
WS-C6506	Catalyst 6506 Chassis
WS-C6509	Catalyst 6509 Chassis
WS-C6509-NEB	Catalyst 6509 Chassis for NEBS Environments
WS-C6513	Catalyst 6513 Chassis
Catalyst 6500 Series Power Supplies	
PWR-950-AC=	Spare 950W AC P/S for Cisco 7603/Cat 6503
PWR-950-DC=	Spare 950W DC P/S for CISCO7603/Cat 6503
PEM-15A-AC=	Spare Pwr Entry Mod for CISCO7603/Cat 6503 (950W AC Pwr Sup)
PEM-DC/3=	Spare DC Power Entry Mod for CISCO7603/Cat 6503
WS-CAC-1000W=	Catalyst 6000 1000W AC Power Supply, Spare
WS-CAC-1300W=	Catalyst 6000 1300W AC Power Supply,Spare
WS-CDC-1300W=	Catalyst 6000 1300W DC Power Supply, Spare
WS-CAC-2500W=	Catalyst 6000 2500W AC Power Supply
WS-CAC-4000W-INT=	4000W AC PowerSupply, International (cableincluded)
WS-CAC-4000W-US=	4000Watt AC Power Supplyfor US (cable attached)
Catalyst 6000 Family Supervisor Engines and Switch Fabric Modules	
WS-X6K-S1A-MSFC2=	Catalyst 6000 Supervisor Engine1-A, 2GE, plus MSFC-2 & PFC
WS-X6K-SUP1A-2GE=	Catalyst 6000 Supervisor Engine1A, Enhanced QoS, 2GE
WS-X6K-SUP1A-PFC=	Catalyst 6000 Supervisor Engine1-A, 2GE, plus PFC
WS-X6K-S2-PFC2=	Catalyst 6500 Supervisor Engine-2, 2GE, plus PFC-2
WS-X6K-S2-MSFC2=	Catalyst 6500 Supervisor Engine-2, 2GE, plus MSFC-2 & PFC-2
WS-X6K-S2U-MSFC2=	Cat6K Sup2 with 256MB DRAM on Sup2 andMSFC2
WS-SUP720=	Cat6500 CEF720 Sup Engine - Integrated Fabric, MSFC3
WS-C6500-SFM=	Catalyst 6500 Switch Fabric Module
WS-X6500-SFM2=	Catalyst 6500 Switch Fabric Module 2, Spare
Catalyst 6500 – 10 Gigabit Ethernet	
WS-X6502-10GE=	Catalyst 6500 10 Gigabit Ethernet Base Module(Req OIM),Spare

Catalyst 6500 – Gigabit Ethernet	
WS-X6148-GE-TX=	Cat6500 48-port 10/100/1000 GE Module, RJ45
WS-X6316-GE-TX=	Catalyst 6000 8-port GE, Enhanced QoS (Req. GBICs)
WS-X6408A-GBIC=	Catalyst 6000 8-port GE, Enhanced QoS (Req. GBICs)
WS-X6416-GBIC=	Catalyst 6000 16-port Gig-Ethernet Mod. (Req. GBICs)
WS-X6416-GE-MT=	Catalyst 6000, 16-port Gigabit EthernetModule, MT-RJ
WS-X6516-GBIC=	Catalyst 6500 16-port GigE Mod: fabric-enabled (Req. GBICs)
WS-X6516A-GBIC=	Catalyst 6500 16-port GigE Mod: fabric-enabled (Req. GBICs)
WS-X6516-GE-TX=	Catalyst 6500 16-port Gig/Copper Module,x-bar
WS-X6816-GBIC=	Catalyst 6500 16-port GigE mod, 2 fab I/F w/DF, (Req GBICs)
Catalyst 6500 – 10/100 Gigabit Ethernet	
WS-X6024-10FL-MT=	Catalyst 6000 24-port 10BASE-FL MT-RJ Module
WS-X6148-RJ-21=	Catalyst 6500 48-Port 10/100 Upgradable to Voice, RJ-21
WS-X6148-RJ21V=	Catalyst 6500 48-port 10/100 Inline Power Module, RJ-21
WS-X6148-RJ-45=	Catalyst 6500 48-Port 10/100, Upgradable to Voice, RJ-45
WS-X6148-RJ45V=	Catalyst 6500 48-port 10/100 Inline Power, RJ-45
WS-X6324-100FX-MM=	Catalyst 6000 24-port 100FX, Enh QoS, MT-RJ, MMF
WS-X6324-100FX-SM=	Catalyst 6000 24-port 100FX, Enh QoS, MT-RJ, SMF
WS-X6348-RJ21V=	Catalyst 6000 48-port 10/100, Inline Power, RJ-21
WS-X6348-RJ-45=	Catalyst 6000 48-port 10/100, Enhanced QoS, RJ-45
WS-X6348-RJ-45V=	Catalyst 6000 48-port 10/100, Inline Power, RJ-45
WS-X6524-100FX-MM=	Catalyst 6500 24-port 100FX, MT-RJ, fabric-enabled
WS-X6548-RJ-21=	Catalyst 6500 48-port 10/100, RJ-21, fabric-enabled
WS-X6548-RJ-45=	Catalyst 6500 48-port 10/100, RJ-45, x-bar
Catalyst 6500 Services Modules	
WS-SVC-CMM=	COMMUNICATION MEDIA MODULE
WS-SVC-CMM-6T1=	6-PORT T1 INTERFACE PORT ADAPTER
WS-SVC-CMM-6E1=	6-PORT E1 INTERFACE PORT ADAPTER
WS-SVC-CSG-1=	Content Services Gateway
WS-SVC-FWM-1-K9=	Firewall blade for Catalyst 6500
WS-SVC-IPSEC-1=	IPSec VPN Security Module for 6500 and 7600 series
WS-SVC-NAM-1=	Catalyst 6500 Network Analysis Module-1
WS-SVC-NAM-2=	Catalyst 6500 Network Analysis Module
WS-SVC-SSL-1-K9=	SSL Module for Catalyst 6500
WS-X6066-SLB-APC=	Catalyst 6500 Content Switching Module
WS-X6381-IDS=	Catalyst 6000 Intrusion Detection System Module
WS-X6608-E1=	Catalyst 6000 8-port Voice E1 and Services Module
WS-X6608-T1=	Catalyst 6000 8-port Voice T1 and Services Module
WS-X6624-FXS=	Catalyst 6000 24-port FXS Analog Station Interface Module
Catalyst 6500 FLEXWAN and OSM Modules	
WS-X6101-OC12-MMF=	Catalyst 6000 1-port Multimode OC-12 ATM Module, Spare
WS-X6101-OC12-SMF=	Catalyst 6000 1-port Single-Mode OC-12 ATM Module, Spare
WS-X6182-2PA=	Catalyst 6000 Flex WAN Module (Supports 2 Port Adapters)
WS-X6516A-GBIC=	Catalyst 6500 16-port GigE Mod: fabric-enabled (Req. GBICs)
Catalyst 6500 Optics	
WS-G5484=	1000BASE-SX Short Wavelength GBIC (Multimode only)
WS-G5486=	1000BASE-LX/LH long haul GBIC (single mode or multimode)
WS-G5487=	1000Base-ZX extended reach GBIC (single mode)
WS-G6483=	Cat 6500 10GBASE-ER Serial 1550nm extended reach OIM (spare)
WS-G6488=	Catalyst 6500 10GBASE-LR Serial 1310nm long haul OIM (spare)
Catalyst 6500 Bundles	
WS-C6503-2GE	Cat6503 chassis w/ Sup1A-2GE (Requires Power Supply)
WS-C6503-PFC2	Cat6503 chassis w/ Sup2-PFC2 (Requires Power Supply)
WS-C6506-2GE	Cat6506 chassis w/ Sup1A-2GE (Requires Power Supply)
WS-C6506-PFC2	Cat6506 chassis w/ Sup2-PFC2 (Requires Power Supply)
WS-C6509-2GE	Cat6509 chassis w/ Sup1A-2GE (Requires Power Supply)
WS-C6509-PFC2	Cat6509 chassis w/ Sup2-PFC2 (Requires Power Supply)
WS-C6509-6816-16	Cat6509 w/S2-MSFC2,SFM2,WS-X6816-GBIC (Req Purch 2 2500W)
WS-C6509-6816-32	Cat6509 w/S2-MSFC2,SFM2,2xWS-X6816-GBIC (Req Purch 2 2500W)
WS-SVC-SSL-CSM-K9=	Catalyst 6500 SSL and CSM Bundle
WS-C6503-FWM-K9	Cisco Catalyst 6503 Firewall Security System
WS-C6506-FWM-K9	Cisco Catalyst 6506 Firewall Security System
WS-C6506-IPSEC-K9	Cisco Catalyst 6506 IPSec VPN System

WS-C6503-IPSEC-K9	Cisco Catalyst 6503 IPsec VPN System
WS-C6506-IPSEC-K9	Cisco Catalyst 6506 IPSec VPN System
Catalyst 6000 Family Accessories	
WS-F6K-MSFC2=	Catalyst 6000 Multilayer Switch Feature Card (MSFCII, Spare
WS-F6K-VPWR=	Catalyst 6000 Voice Power Feature Card for WS-X6348-RJ-45
WS-F6K-DFC=	Distributed Forwarding Card
WS-C6X09-RACK=	Catalyst 6x00 Rack Mount Kit and Cable Organizer
WS-C6K-6SLOT-FAN=	Catalyst 6000, Fan Tray for 6-slot Systems
WS-C6X06-RACK=	Catalyst 6x06, Rack Mount Kit and Cable Organizer
Catalyst 6000 Family Software and Element Management Software (EMS)	
WS-C6513-EMS-LIC=	Catalyst 6513 RMON Agent License
WS-C6X09-EMS-LIC	Catalyst 6x09 RMON Agent License
WS-C6X06-EMS-LIC	Catalyst 6x06 RMON Agent License (also available for Cat6x09)
FRC6-MSM-IPX=	Catalyst 6000 MSM IPX Feature Set License, Spare
FR-IRC6=	Catalyst 6000 Family InterDomain Routing Feature License
S6MSFC2A-12102E=	Catalyst 6000 MSFC2 IOS Enterprise (also available in images with VIP, Desktop, IP/IPX, etc.)
SC6K-SUP2-6.1.1	Catalyst 6000 Supervisor 2 Flash Image, Rel 6.1(1)
SC6K-SUP2CV-6.1.1	Cat6K Supervisor 2 Flash Image w/CiscoView, Rel 6.1(1)
SC6K-SUP2K9-6.1.1	Catalyst 6000 Supervisor 2 Flash Image w/SSH, Rel 6.1(1)
SC6K-S2K9CV-6.1.1	Cat6K Sup 2 Flash Image w/CiscoView & w/SSH, Rel 6.1(1)
S6SUP22A-12105E	Catalyst 6000 Sup2/MSFC IOS Enterprise (also available in images with Desktop, IP, IP/IPX)
SC6K-SUP-5.4.4=	Catalyst 6000 Supervisor Flash Image, Release 5.4(4)
EMS-6500-025C-1.0=	6500 EMS 25 Chassis RTU License-6750 Per Chassis List
EMS-6500-100C-1.0=	6500 EMS 100 Chassis RTU License-6000 Per Chassis List
EMS-6500-250C-1.0=	6500 EMS 250 Chassis RTU License-5250 Per Chassis List
EMS-6500-500C-1.0=	6500 EMS 500 Chassis RTU License-4500 Per Chassis List
Catalyst 6000 Family Memory Options	
MEM-C6K-FLC16M=	Catalyst 6000, Supervisor PCMCIA 16MB Flash Memory Card
MEM-C6K-FLC24M=	Cat 6000 Sup PCMCIA Flash Memory Card, 24 MB Spare
MEM-MSFC-128MB=	Catalyst 6000 MSFC Mem, 128 MB DRAM Option
MEM-C6K-WAN-128M=	Catalyst 6000 WAN Module Memory, 128 MB
MEM-MSFC2-256MB=	MSFC2 256MB Memory Option (also available in 512 MB)
MEM-DFC-256MB=	Catalyst 6500 256 MB spare for DFC
MEM-DFC-512MB=	Catalyst 6500 512 MB option for DFC
MEM-S2-256MB=	256 MB DRAM spare for Sup2
Catalyst 6000 Family Packaged SMARTnet Maintenance 8x5xNBD	
CON-SNT-PKG12	Catalyst 6503 L2 Bundle SMARTnetMaintenance 8x5xNBD
CON-SNT-PKG14	Catalyst 6506 L2 Bundle SMARTnetMaintenance 8x5xNBD
CON-SNT-PKG15	Catalyst 6509 L2 Bundle SMARTnetMaintenance 8x5xNBD
CON-SNT-PKG16	Catalyst 6006 and 6506, Packaged SMARTnet Maintenance 8x5xNBD
CON-SNT-PKG17	Catalyst 6009 and 6509, Packaged SMARTnet Maintenance 8x5xNBD

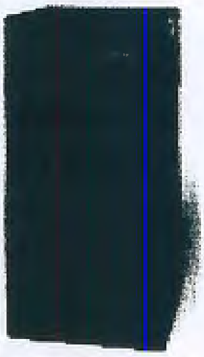
[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Catalyst 6000 Family Web site: **http://www.cisco.com/go/6000**

7416
3

Cisco Catalyst 8500 Multiservice Switch Routers



The Catalyst 8500 family multiservice switch routers integrate multiservice ATM switching with wire-speed multiprotocol routing for Gigabit Ethernet and Fast Ethernet into a single platform that also supports advanced Cisco IOS services for QoS and security. This family delivers enterprise MAN/WAN and Service Provider multiservice edge solutions with scalable performance, lower cost of ownership, and offer multiple interface options in a modular chassis. The Catalyst 8500 series consists of the modular Catalyst 8510 (10-Gbps, 5-slot) switch and the modular Catalyst 8540 (40-Gbps, 13-slot) switch. Both switches implement Cisco IOS Software to provide a variety of network services including reliability, security, management, and QoS with CiscoAssure policy networking.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 8540 and Catalyst 8510	• Integrated 10/100 FE, GE, and ATM • Flexible ATM interfaces (T1/E1, IMA, DS3/E3, OC-3, OC-12, and OC-48) • Frame relay and circuit emulation services • Wire-speed performance • Multiservice MAN/WAN applications • Multiservice Edge solutions • Voice, data, and video solutions • MPLS VPN

Key Features

- Ideal for integrated multiservice ATM switching with wire-speed multiprotocol routing for gigabit Ethernet (L3eATM or Layer 3 enabled ATM)
- Ideal for aggregating multiprotocol traffic from multiple wiring closets or from workgroup switches such as the Catalyst 5000 or distribution/server aggregation switches such as the Catalyst 6000 Family
- Provides nonblocking routing for IP, IPX, and IP multicast while also offering wire-speed Layer 2 switching for nonroutable protocols such as NetBIOS and DECnet local-area transport (LAT)
- Aggregate throughput of up to 24 million packets per second (pps) for non-blocking, wirespeed Layer 3 switching

Competitive Products

- Foundry: Big Iron
- Lucent: PSAX 1250 and 2300
- Marconi: ASX 1000, 1200, and 4000
- Alcatel: Omniswitch

Specifications

Feature	Catalyst 8510	Catalyst 8540
Modular Slots	5	13
Available Modules	See Part Numbers and Ordering information for a partial parts list	
Backplane	10 Gbps	40 Gbps
Throughput Performance	6 Mpps	24 Mpps
MAN / WAN	POS / ATM Uplink	POS / ATM Uplink
Dimensions (HxWxD)	10.5 x 17.2 x 18.14 in.	25.25 x 17.3 x 18.25 in.

7714 3

Selected Part Numbers and Ordering Information[1]

Catalyst 8540—Common Equipment

C8540MSR-SKIT-AC	C8540 MSR Starter Kit w/ Stratum 4Clock Module—AC Power(also available in DC Power)
C8545MSR-MRP4CLK=	C8540 MSR Multiservice Route Processor (spare)
C8545MSR-MRP3CLK=	C8540 MSR Route ProcessorStratum 3 (spare)
C8546MSR-MSP-FCL=	C8540 MSR Switch Processor with ATM FC (spare)
C8540CSR-SKIT-AC	Catalyst 8540 CSR Starter Kit with AC Power (also available in DC Power)
C8541CSR-RP=	Catalyst 8540 CSR Route Processor(spare)
C8542CSR-SP=	Catalyst 8540 CSR Switch Processor (spare)
C8540-CHAS13=	Catalyst 8540 - Chassis (spare)
C8540-PWR-AC=	C8540 Power Supply—AC (also available in DC Power)

Catalyst 8510—Common Equipment

C8510MSR-SKIT-AC	Catalyst 8510 MSR Starter Kit with AC Power (alsoavailable as -DC for DC Power
C8515-MSRP=	C8510 Multiservice Switch Route Processor (spare)
C8510CSR-SKIT-AC	Catalyst 8510 CSR Starter Kit with AC Power (also available as -DC for DC Power)
C8510-SRP=	C8510 Layer 3 Switch Route Processor (spare)
C8510-CHAS5=	Catalyst 8510 - Chassis (spare)
C8510-PWR-AC=	C8510 power supply, AC (spare) (alsoavailable in DC power)

Catalyst 8500 Family—ATM Router Module Equipment

C8540-ARM-64K=	C8540 ATM Router Module 64K (also available for 8510)
C8540-ARM2=	C8540 EnhancedATM Router Module (spare)

Catalyst 8500—Layer 3 Modules and ATM Interface Modules and Uplinks

C85EGE-2X-16K=	C8540 2-port EnhancedGE 16K (also available in 64K and 256K)
C85GE-8X-64K=	C8540 8-port GE 64K
C85FE-16TACL-64K=	C8540 16-port 10/100 RJ-45 w/ACL 64K
C85FE-16FACL-64K=	C8540 16-port 100-FX MT-RJ w/ACL 64K
C8540-ACL=	C8540 ACL Daughter Card (also available for C8510/LS1010)
C85GE-1X-16K=	C8510/LS1010 1-port Gigabit Ethernet16K (also available in 64K)
C85FE-8T-64K=	C8510/LS1010 8-port 10/100 RJ-45 64K
C85FE-8F-64K=	C8510/LS1010 8-port 100-FX MT-RJ 64K
C85MS-1F4S-OC48SS=	C8540 1-port OC-48c/STM-16 SMF-IR+4-port OC-12 SMF
C85MS-1F4M-OC48SS=	C8540 1-port OC-48c/STM-16 SMF-IR+4-port OC-12 MMF
C85MS-4F-OC12SS=	C8540 4-port OC-12c/STM-4 SMF
C85MS-4F-OC12MM=	C8540 4-port OC-12c/STM-4 MMF
C85MS-16F-OC3MM=	C8540 16-port OC-3c/STM-1 MMF (spare)
C85MS-16F-OC3SM=	C8540 16-port OC-3c/STM-1 SMF-LR (spare)

Catalyst 8500—Port Adapter Modules

C85MS-SCAM-2P=	C8540 SuperCAM for Port Adapter Modules (spare)
C8510TSCAM-2P=	CS8510/LS1010 Traffic Shaping Carrier Access Modules (spare)
WATM-CAM-2P=	C8510 / LS1010 Carrier Modules (spare)
WAI-T1C-4RJ48=	4 Port T1 (circuit emulation) RJ-48 PAM (also available in El andin E1 BNC)
C85MS-4E1-FRRJ48=	C8500 4-port E1 Frame-Relay/FUNI PAM (spare)
WAI-OC3-4MM=	4 Port OC-3c/STM-1 MMF PAM (also available in SMF-IR & SMF-LR)
WAI-OC3-1S3M=	OC-3c/STM-1 Mix PAM, 1-port SMF-IR + 3-port MMF (spare)
WAI-OC12-1MM=	1 Port OC-12c/STM-4c MMF PAM (also available in SMF-IR and SMF-LR)
WAI-T3-4BNC=	4 Port DS-3 PAM (spare and in E3 BNC)
C85MS-8T1-IMA=	C8500MSR/LS1010 8-port TI IMA PAM (also available in E1 120 ohm)
WAI-T1-4RJ48=	4 Port T1 (ATM) RJ-48 PAM (spare also available in E1 and E1 BNC E1)

Catalyst 8500 Software Feature License Options

FR-8510-TAGSW=	C8510 Tag Switching upgrade license (also available with HPNNI and HPNNI + Tag Switching)
FR-8540MSR-HPNNI=	Cat 8540MSR—Hierarchical PNNI License (also available with Tag Switching)

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Catalyst 8500 series Web site: **http://www.cisco.com/go/8500**

CHAPTER 3 7712

Wireless LAN Products

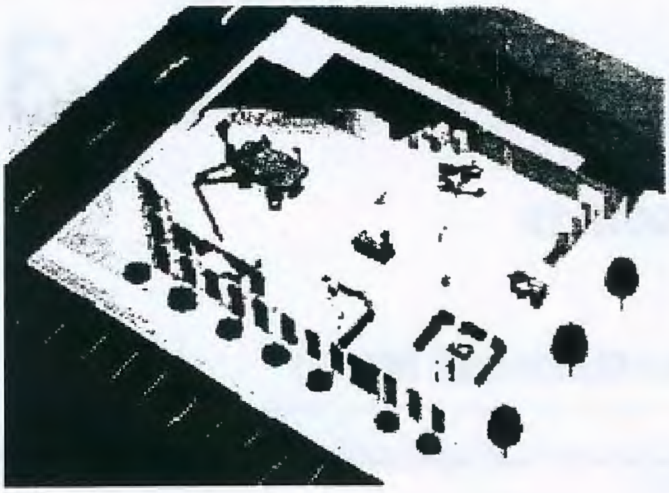
Wireless LAN Products at a Glance (IEEE 802.11b)

Product	Features	Page
Cisco Aironet 1200 Series Access Points	• Offers investment protection and a smooth migration path to future technologies through a dual band radio design • Delivers an enterprise class security solution with the IEEE 802.11x-based Cisco Wireless Security Suite • Industry-leading security, network management, throughput and software feature set • Support for both line power over Ethernet and localpower	3-2
Cisco Aironet 1100 Series Access Point	• Single 802.11b radio, upgradable to 802.11g • Provides end-to-endsolution support for Intelligent NetworkServices • Delivers an enterprise class security solution with the IEEE 802.11x-based Cisco Wireless Security Suite • Support for both line power over Ethernet and local power • Cost effective, yet feature-rich	3-5
Cisco Aironet 5 GHz 54 Mbps Wireless LAN Client Adapter	• IEEE 802.11a-compliant CardBus adapterthat operatesin the UNII-1 and UNII-2 bands • Complementsthe Cisco Aironet 1200 Series 802.11a Access Point, providing a solution that combines performance and mobility with the security and manageability that enterprises require	3-6
Cisco Aironet 350 Series Client Adapters	• Superior range and throughput • Secure networkcommunications • World mode for internationalroaming • PCMCIA card and PCI form factors • IEEE 802.11b	3-8
Cisco Aironet 350 Series Workgroup Bridge	• Driverless installation of up to eight Ethernet-enabled devices • Optimum wireless performance and range • Standards-based centralized security • IEEE 802.11b	3-10
Cisco Aironet 350 Series Wireless Bridge	• High-speed, high-power radios, delivering building-to-building links of up to 25 miles (40.2 km) • A metal case for durability and plenum rating • Supports both pointto-point and point-to-multipoint configurations • Broad range of support antennas • Simplified installation, improved performance, and upgradeablefirmware, ensuring investment protection • IEEE 802.11b	3-12
Cisco Aironet Antennas and Accessories	• A wide array of options • FCC-approved directional and omni-directional antennas • Low-loss cable, mounting hardware, and other accessories available	3-14
CiscoWorks Wireless LAN Solution Engine	A hardware-based wireless LAN managementsolution that provides template-based configuration with user-defined groupsto effectively manage a large numberof accesspoints and bridges. • Monitors LEAP authentication servers • Enhancessecurity management through misconfiguration detection on acces points and bridges	9-23

CHAPTER 3 WIRELESS LAN PRODUCTS

Af

Sample Wireless LAN Solution Overview—In-Building or Site-to-Site



Enterprise, Small/Medium Business Applications

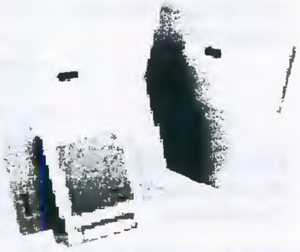
Service common areas for mobile workers
Support employees working in multiple offices
Cost effective, quick network deployment for temporary or leased offices

Sample Vertical Markets

Healthcare, retail, government
Public Access
Multiple Tenant/Dwelling Units
Airports, Hotels, Convention Centers
Education:K-12 and Universities

7711
3

Cisco Aironet 1200 Series Access Points



The Cisco Aironet 1200 Series Access Point sets the enterprise standard for next-generation high performance secure, manageable, and reliable wireless local-area networks (WLANs) while also providing investment protection because of its upgrade capability and compatibility with current standards. The modular design of the Cisco Aironet 1200 supports IEEE 802.11a and 802.11b technologies in both single-and dual-mode operation. You can configure the Cisco Aironet 1200 to meet customer-specific requirements at the time of purchase and then reconfigure and upgrade the product in the field as these requirements evolve.

The Cisco Aironet 1200 Series protects current and future network infrastructure investments. Compliant with IEEE 802.11a and 802.11b standards, The 802.11a radio supports data rates of up to 54 Mbps and eight non-overlapping channels that offer high performance as well as maximum capacity and scalability. The 802.11b radio provides data rates up to 11 Mbps and three non-overlapping channels to support widely deployed 802.11b clients. The Mini-PCI form factor of the 802.11b radio allows for upgrade to higher-speed 2.4 GHz technologies such as the draft IEEE 802.11g standard.The Cisco Aironet 1200 Series extends end-to-end intelligent networking to the wireless access point with support for enterprise-class virtual LANs (VLANs) and quality of service (QoS). An ideal choice for enterprise installations, the Cisco Aironet 1200 Series can manage up to 16 VLANs, which allows customers to differentiate LAN policies and services, such as security and QoS, for different users. Traffic to and from wireless clients with varying security capabilities can be segregated into VLANs with varying security policies.

Wireless LAN security is a primary concern. The Cisco Aironet 1200 Series secures the enterprise network with a scalable and manageable system featuring the award-winning Cisco Wireless Security Suite. Based on the 802.11x standard for port-based network access, the Cisco Wireless Security Suite takes advantage of the Extensible Authentication Protocol (EAP) framework for user-based authentication.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 1200 Series Access Point	• IT Professionals or business executives want mobility within the enterprise to increase productivity, as an addition or alternative to wired networks. • Business owners or IT directors need flexibility for frequent LAN wiring changes, either throughout the site or in selected areas. • Any company whose site is not conducive to LAN wiring because of building or budget limitations, such as older buildings, leased space or temporary sites.

Key Features

- Offers investment protection because of its upgrade capability and compatibility with current standards
- Delivers an enterprise class security solution with the IEEE 802.11x-based Cisco Wireless Security Suite
- Industry-leading security, network management, and software feature set
- Support for both inline power over Ethernet or local power
- Simultaneous support for both IEEE 802.11b and IEEE 802.11a

Specifications

Feature	Cisco Aironet 1200 Series Access Points with 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Data Rates Supported	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, and 11 Mbps	Same as 802.11a and 802.11b combined
Uplink	Autosensing 802.3 10/100BaseT Ethernet	Autosensing 802.3 10/100BaseT Ethernet	Same as 802.11a and 802.11b combined
Form Factor	CardBus (32-bit)	Mini-PCI	Same as 802.11a and 802.11b combined
Frequency Band	5.15 to 5.35 GHz (FCC UNII 1 and UNII 2), 5.15 to 5.25 GHz (TELEC),5.15 to 5.25 GHz (Singapore),5.25 to 5.35 GHz (Taiwan)	2.412 to 2.462 GHz (FCC),2.412 to 2.472 GHz (ETSI),2.412 to 2.484 GHz (TELEC),2.412 to 2.462 GHz (MII),2.422 to 2.452 GHz (Israel)	Same as 802.11a and 802.11b combined
Wireless Medium	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS)	Same as 802.11a and 802.11b combined
Modulation	(OFDM subcarrier);BPSK @ 6 and 9 Mbps; QPSK @ 12 and 18 Mbps; 16-QAM @ 24 and 36 Mbps;64-QAM @ 48 and 54 Mbps	DBPSK @1 Mbps; DQPSK @ 2 Mbps; CCK @ 5.5 and 11 Mbps	Same as 802.11a and 802.11b combined
Operating Channels	FCC: 8;TELEC (Japan): 4; Singapore: 4; Taiwan: 4	ETSI: 13; Israel: 7; North America: 11; TELEC (Japan): 14; MII: 11	Same as 802.11a and 802.11b combined
Nonoverlapping Channels	Eight (FCC only); Four (Japan, Singapore, Taiwan)	Three	Eleven
Available Transmit Power Settings[1]	40 mW (16 dBm);20 mW (13 dBm);10 mW (10 dBm);5 mW (7 dBm); Maximum power setting will vary according to individual country regulations.	100 Mw (20 dBm); 5 Mw (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm); Maximum power setting will vary according to individual country regulations	Same as 802.11a and 802.11b combined
Range (typical @ maximum power setting, 2.2 dBi gain diversity dipole antenna)	Omni directional Antenna: Indoor: 60 ft (18m)@ 54 Mbps, 130 ft (40m) @ 18 Mbps, 170 ft (52m) @ 6 Mbps; Outdoor: 100 ft (30m) @ 54 Mbps, 600 ft (183m) @ 18 Mbps, 1000 (304m) ft @ 6 Mbps; Patch Antenna: Indoor: 70 ft (21m) @ 54 Mbps, 150 ft (45m) @ 18 Mbps, 200 ft (61m) @ 6 Mbps; Outdoor: 120 ft (36m) @ 54 Mbps, 700 ft (213m) @ 18 Mbps; 1200 ft (355m) @ 6 Mbps	IIndoor:130 ft (40m) @ 11 Mbps; 350 ft (107m) @ 1 Mbps Outdoor: 800 ft (244m) @ 11 Mbps; 2000 ft (610m) @ 1Mbps	Same as 802.11a and 802.11b combined
SMTP Compliance	MIB I and MIB II	MIB I and MIB II	MIB I and MIB II
Antenna	Integrated 6 dBi diversity patch (55 degree horizontal, 55 degree vertical beamwidths, 5 dBi diversity omnidirectional with 360 degree horizontal and 40 degree vertical beamwidths	Two RP-TNC connectors (antennas optional, none supplied with unit)	5 GHz: Integrated 6 dBi diversity patch (55 degree horizontal, 55 degree vertical beamwidths, 5 dBi diversity omnidirectional with 360 degree horizontal and 40 vertical beamwidths; 2.4 GHz: Two RP-TNC connectors (antennas optional, none supplied with unit)

7709
3

Feature	Cisco Aironet 1200 Series Access Points with 802.11a radio installed	With 802.11b radio installed	With both 802.11a and 802.11b radio installed
Security architecture client authentication	Cisco Wireless Security Suite including: Authentication: 802.11x support including LEAP, PEAP, EAP-TLS, EAP-TTLS, and EAP-SIM to yield mutual authentication and dynamic, per-user, per-session WEP keys; MAC address and by standard 802.11 authentication mechanisms Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; Pre-standard TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation	Cisco Wireless Security Suite including: Authentication: 802.11x support including LEAP, PEAP, EAP-TLS, EAP-TTLS, and EAP-SIM to yield mutual authentication and dynamic, per-user, per-session WEP keys; MAC address and by standard 802.11 authentication mechanisms Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; Pre-standard TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation	Same as 802.11a and 802.11b combined
Software Image Network and Inventory support	CiscoWorks RME[2], CiscoWorks SWIM[3]	CiscoWorks RME[2], CiscoWorks SWIM[3]	CiscoWorks RME[2], CiscoWorks SWIM[3]
Remote configuration support	BOOTP, DHCP, Telnet, HTTP, FTP, TFTP, and SNMP	Telnet, HTTP, FTP, TFTP, and SNMP	Telnet, HTTP, FTP, TFTP,and SNMP
Local configuration	Direct consoled port (RJ-45 interface)	Direct consoled port (RJ-45 interface)	Direct consoled port (RJ-45 interface)
Environmental	-4° to 122°F (-20° to 50°C), 10 to 90% humidity (noncondensing)	-4° to 131°F (-20° to 55°C), 10 to 90% humidity (noncondensing)	-4° to 122°F (-20° to 50°C), 10 to 90% humidity (noncondensing)
Input Power Requirements	90 to 240 VAC +/- 10% (power supply);48 VDC +/- 10%(device)	90 to 240 VAC +/- 10% (power supply);48 VDC +/- 10%(device)	90 to 240 VAC +/- 10% (power supply);48 VDC +/- 10%(device)
Power Draw	8 watts, RMS	6 watts, RMS	11 watts, RMS
Warranty	One year	One year	One year

1. Management Information Base
2. CiscoWorks Resource Manager Essentials
3. Software Image Manager

Selected Part Numbers and Ordering Information[1]

1200 Series Access Points	
AIR-AP1200	AP Platform, Cardbus and MPCI Slots (no radio), Enet Uplink
AIR-AP1220B-A-K9	802.11b AP w/Avail CBus Slot, FCC Cnfg
AIR-AP1220B-E-K9	802.11b AP w/Avail CBus Slot, ETSI Cnfg
AIR-AP1220A-J-K9	802.11a AP w/Avail MPCI Slot, Enet Uplink, TELEC Cnfg
AIR-AP1220B-J-K9	802.11b AP w/Avail CBus Slot, Japan Cnfg
1230 Series Access Points	
AIR-AP1210	IOS based AP Platform, Cardbus and MPCI Slots (no radio), Enet Uplink
AIR-AP1230B-A-K9	IOS based 802.11b AP w/Avail CBus Slot, FCC Cnfg
AIR-AP1230B-E-K9	IOS based 802.11b AP w/Avail CBus Slot, ETSI Cnfg
AIR-AP1230A-J-K9	IOS based 802.11a AP w/Avail MPCI Slot, Enet Uplink, TELEC Cnfg
AIR-AP1230B-J-K9 I	OS based 802.11b AP w/Avail CBus Slot, Japan Cnfg

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the Distribution Product Reference Guide at: http://www.cisco.com/dprg (limited country availability)

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 1100 Series Access Points

The Cisco Aironet® 1100 Series Access Point provides a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals.

Taking advantage of the Cisco Wireless Security Suite for the strongest enterprise security available and of Cisco IOS® Software for ease-of-use and familiarity, the Cisco Aironet 1100 Series Access Point delivers manageability, performance, investment protection, and scalability in a cost-effective package with a low total cost of ownership. The Cisco Aironet 1100 Series features a single, upgradable 802.11b radio, integrated diversity dipole antennas, and an innovative mounting system for easy installation in a variety of locations and orientations.

The first access point based on Cisco IOS Software, the Cisco Aironet 1100 Series extends end-to-end intelligent networking to the wireless access point. Cisco command-line interface (CLI) allows customers to quickly and consistently implement extended capabilities available in Cisco IOS Software. Customers can manage and standardize their networks using tools they have developed internally for their Cisco routers and switches.

Enterprise-class features including virtual LANs (VLANs), quality of service (QoS), and proxy mobile Internet Protocol (IP) make the Cisco Aironet 1100 Series ideal for enterprise installations. The Cisco Aironet 1100 Series also supports standard Cisco Aironet features such as hot-standby and load balancing, allowing enterprises to implement intelligent, reliable network services.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 1100 Series Access Point	• A cost-effective and upgradable WLAN solution that combines the mobility and flexibility of a WLAN solution with the enterprise-class features required by a business LAN. Want an off the shelf WLAN solution that does not require simultaneous dual band operation, or the additional range offered by high-gain antennas.

Key Features

- Single 802.11b radio, upgradable to 802.11g
- Provides end-to-end solution support for Intelligent Network Services
- Variety of mounting options
- Cost effective, yet feature-rich

Specifications

Feature	Cisco Aironet 1100 Series Access Points
Data Rates Supported	1, 2, 5.5, 11 Mbps
Network standard	IEEE 802.11b
Uplink	Autosensing 802.3 10/100BaseT Ethernet
Frequency Band	2.412 to 2.462 GHz (FCC); 2.412 to 2.472 GHz (ETSI); 2.422 to 2.452 GHz (Israel); 2.412 to 2.484 GHz (TELEC)
Network architecture type	Infrastructure, star topology
Wireless Medium	Direct Sequence Spread Spectrum (DSSS)
Modulation	DBPSK @ 1 Mbps; DQPSK @ 2 Mbps; CCK @ 5.5 and 11 Mbps
Operating Channels	ETSI: 13; Israel: 7; Americas: 11; TELEC (Japan): 14
Nonoverlapping Channels	Three
Receive sensitivity	1 Mbps: -94 dBm; 2 Mbps: -91 dBm; 5.5 Mbps: -89 dBm;11 Mbps: -85 dBm

Feature	Cisco Aironet 1100 Series Access Points
Available Transmit Power Settings[1]	100 mW (20 dBm); 50 mW (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm) Maximum power setting will vary according to individual country regulations
Range (typical @ maximum power setting, 2.2 dBi gain diversity dipole antenna)	Indoor: 150 ft (45 m) @ 11 Mbps; 400 ft (122 m) @ 1 MbpsOutdoor: 800 ft (244 m) @ 11 Mbps; 2000 ft (610 m) @ 1 Mbps
SMTP Compliance	MIB I and MIB II
Antenna	Integrated 2.2 dBi diversity dipole antennas
Security architecture client authentication	Cisco Wireless Security Suite including:Authentication: 802.11x support including LEAP, PEAP, EAP-TLS, EAP-TTLS and EAP-SIM to yield mutual authentication and dynamic, per-user, per-session WEP keys; MAC address and by standard 802.11 authentication mechanisms Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; Pre-standard TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation
Software Image Network and Inventory support	CiscoWorks CiscoView, Resource Manager Essentials, and Campus Manager
Remote configuration support	BOOTP, DHCP, Telnet, HTTP, FTP, TFTP, and SNMP
Dimensions	4.1 in. (10.4 cm) wide; 8.1 in. (20.5 cm) high; 1.5 in. (3.8 cm) deep
Weight	10.5 oz. (297 g)
Environmental	32° to 104° F (0° to 40° C); 10-90% humidity (noncondensing)
System Memory	16 MB RAM; 8 MB Flash
Input Power Requirements	100 to 240 VAC 50 to 60Hz (power supply); 33 to 57 VDC (device)
Power Draw	4.9 watts, RMS
Warranty	One year

[1] Management Information Base

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 5 GHz 54 Mbps Wireless Client Adapter

The Cisco Aironet® 5 GHz 54 Mbps Wireless LAN client adapter is an Institute of Electrical and Electronic Engineers (IEEE) 802.11a-compliant CardBus adapter that operates in the UNII-1 and UNII-2 bands. The client adapter complements the Cisco Aironet 1200 Series 802.11a Access Point, providing a solution that combines performance and mobility with the security and manageability that enterprises require.

Wireless LAN client adapters can increase productivity by enabling mobile users to have network and Internet access anywhere within a building that is equipped with a wireless network infrastructure. Wireless client adapters connect a variety of devices to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with access points. With this client adapter, you can quickly add new employees to a network, support temporary workgroups, or enable Internet access in conference rooms or other meeting spaces. And the Cisco Aironet client solution is easy to use, making the benefits of wireless mobility completely transparent.

With Cisco, you can confidently deploy a wireless solution that provides robust enterprise-class security. All Cisco Aironet products feature the award-winning Cisco Wireless Security Suite, which is based on the IEEE 802.11x standard for port-based network access.

The Cisco Wireless Security Suite takes advantage of the Extensible Authentication Protocol (EAP) framework for user-based authentication. It supports a variety of 802.11x authentication types including EAP Cisco Wireless (LEAP) and EAP-Transport Layer Security (EAP-TLS).

The Cisco Aironet Client Utility (ACU), with an intuitive graphical user interface, provides an easy way to configure, monitor, and manage the Cisco Aironet 5 GHz Wireless LAN Client Adapter. The ACU includes site-survey tools that present easy-to-understand detailed graphical information to assist in the placement of access points. Profile Manager allows you to create specific profile settings for various environments, such as the office or home, making it simple for telecommuters and business travelers to move from one environment to another.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 5 GHz 54Mbps Wireless LAN Client Adapters	• Industry leading security: IEEE 802.11x support, including LEAP and EAP-TLS, for mutual authentication and dynamic per-user, per session WEP keys • Multiple transmit power settings (20 mW/(13 dBm), 10 mW/(10 dBm), and 5 mW (7 dBm) • End-to-end Cisco branded solution

Key Features

- IEEE 802.11a-compliant CardBus adapter that operates in the UNII-1 and UNII-2 bands
- Complements the Cisco Aironet 1200 Series 802.11a Access Point, providing a solution that combines performance and mobility with the security and manageability that enterprises require

Specifications

Feature	Cisco Aironet 5 GHz 54 Mbps Wireless Client Adapter
Form Factor	CardBus Type II
Interface	32-bit CardBus (PCI)
Operational voltage	3.3 V (+/- 0.33 V)
LED	Status (green) and Activity (amber)
Data Rates Supported	6, 9, 12, 18, 24, 36, 48, 54 Mbps (configurable as fixed or auto selecting to extend range)
Network Standard	IEEE 802.11a
Frequency Band	5.15 to 5.35 GHz (FCC UNII 1 and UNII 2); 5.15 to 5.25 GHz (TELEC); 5.15 to 5.25 GHz (Singapore); 5.25 to 5.35 GHz (Taiwan)
Network architecture type	Infrastructure, star topology
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Wireless Medium	Orthogonal Frequency Division Multiplexing (OFDM)
Modulation	(OFDM sub-carrier); BPSK @ 6 and 9 Mbps; QPSK @ 12 and 18 Mbps; 16-QAM @ 24 and 36 Mbps; 64-QAM @ 48 and 54 Mbps
Operating Channels	FCC: 8 channels (UNII-1 4 channels and UNII-2 4 channels); 4 channels for Japan, Singapore, and Taiwan
Available Transmit Power Settings[1]	20 mW (13 dBm);10 mW (10 dBm); 5 mW (7 dBm) Maximum power setting will vary according to individual country regulations.
Current steady state (typical)	Transmit: 520 mA; Receive: 580 mA; Sleep: 20 mA
Range	Omni directional Antenna: Indoor: 60 ft (18m)@ 54 Mbps, 130 ft (40m) @ 18 Mbps, 170 ft (52m) @ 6 Mbps Outdoor: 100 ft (30m) @ 54 Mbps, 600 ft (183m) @ 18 Mbps, 1000 (304m) @ 6 Mbps Patch Antenna: Indoor: 70 ft (21m) @ 54 Mbps, 150 ft (45m) @ 18 Mbps, 200 ft (61m) @ 6 Mbps Outdoor: 120 ft (36m) @ 54 Mbps, 700 ft (213m) @ 18 Mbps, 1200 ft (355m) @ 6 Mbps
Power Management	3 levels of power consumption available, including: CAM (Constantly Awake Mode), Fast PSP (Power Save Mode), Max PSP (Maximum Power Savings)
Antenna	Integrated 5dBi gain patch antenna

Feature	Cisco Aironet 5 GHz 54 Mbps Wireless Client Adapter
Security architecture client authentication	Cisco Wireless Security Suite including: Authentication: 802.11x support for LEAP and EAP-TLS to yield mutual authentication and dynamic, per-user, per-session WEP keys; MAC address and by standard 802.11 authentication mechanisms Encryption: Support for static and dynamic IEEE 802.11 WEP keys of 40 bits and 128 bits; Pre-standard TKIP WEP enhancements: key hashing (per-packet keying), message integrity check (MIC) and broadcast key rotation
Drivers	Windows, 98/98SE, Windows ME, Windows 2000 and Windows XP
Environmental	-30° to 70°C; 95% humidity (noncondensing)
Warranty	One year

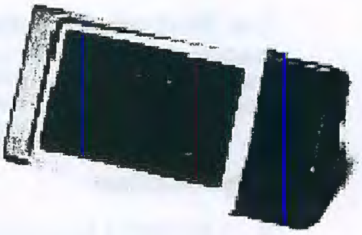
[1] Management Information Base

7705.3

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 350 Series Client Adapters



Wireless client adapters are the key to adding mobility and flexibility to an enterprise—increasing productivity by enabling users to have network and Internet access anywhere within a building without the limitation of wires. The Cisco Aironet 350 Series 802.11b Client Adapters are a complement to Aironet 350 Series infrastructure devices, providing an enterprise-ready solution that combines mobility with the performance, security, and manageability that people have come to expect from Cisco. Wireless client adapters connect a variety of devices to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with Access Points. Available in PC Card (PCMCIA) and Peripheral Component Interconnect (PCI) form factors, Cisco Aironet 350 Series Client Adapters quickly connect desktop and mobile computing devices wirelessly to all network resources. With this product, you can instantly add new employees to the network, support temporary workgroups, or enable Internet access in conference rooms or other meeting spaces.

Cisco Aironet 350 Series Client Adapters deliver superior range, reliability, and performance for business users needing information access anytime, anywhere. Combined with Cisco Aironet unique security services, this product ensures that business-critical information is secure. Most importantly, the Cisco client solution is easy to use, making the benefits of wireless mobility completely transparent.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 350 Series Client Adapters	• IT Professionals or business executives want mobility within the enterprise to increase productivity, as an addition or alternative to wired networks. • Business owners or IT directors need flexibility for frequent LAN wiring changes, either throughout the site or in selected areas. • Any company whose site is not conducive to LAN wiring because of building or budget limitations, such as older buildings, leased space or temporary sites.

Key Features

- Superior range and throughput for IEEE 802.11b networks
- Secure network communications
- World mode for international roaming
- Full-featured utilities for easy configuration and management
- Compliance with the IEEE 802.11b high-rate standard
- Support for all popular operating systems

Specifications

Feature	Cisco Aironet 350 Series Client Adapters
Data Rates Supported	1, 2, 5.5, and 11 Mbps
Network Standard	IEEE 802.11b
System Interface	AIR-PCM35x: PC Card (PCMCIA) Type II AIR-PCI 35x: peripheral component interconnect (PCI) Bus
Frequency Band	2.4 to 2.4897 GHz
Network Architecture Types	Infrastructure and ad hoc
Wireless Medium	Direct Sequence Spread Spectrum (DSSS)
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	DBPSK @1 Mbps; DQPSK @ 2 Mbps; CCK @ 5.5 and 11 Mbps
Operating Channels	North America: 11; ETSI: 13; Japan: 14
Nonoverlapping Channels	Three
Receive Sensitivity	1 Mbps: -94 dBm 2 Mbps: -91 dBm 5.5 Mbps: -89 dBm 11 Mbps: -85 dBm
Delay Spread	1 Mbps: 500 ns; 2 Mbps: 400 ns; 5.5 Mbps: 300 ns; 11 Mbps: 140 ns
Available Transmit Power Settings[1]	100 mW (20 dBm); 50 mW (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm)
Range (typical)	Indoor: 130 ft (40 m) @ 11 Mbps; 350 ft (107 m) @ 1 Mbps Outdoor: 800 ft (244 m) @ 11 Mbps; 2000 ft (610 m) @ 1 Mbps
Compliance	Operates license free under FCC Part 15 and complies as a Class B device; complies with DOC regulations; complies with ETS 300.328, FTZ 2100, and MPT 1349 standards
Operating Systems Supported	Windows 95, 98, NT 4.0, 2000, ME, XP, CE 2.11, CE 3.0, Mac OS 9.x, and Linux
Antenna	AIR-PCM35x: Integrated diversity dipoles AIR-LMC35x: Two MMCX connectors (antennas optional, none supplied with unit) AIR-PCI35x: External, removable 2.2 dBi Dipole with RP-TNC Connector
Encryption Key Length	128-bit
Authentication Type	EAP-Cisco Wireless LEAP
Status Indicators	Link Status and Link Activity
Dimensions (W x D x H)	AIR-PCM35x: 2.13 in. (5.4 cm) x 4.37 in. (11.1 cm) x 0.1 in. (0.3 cm) AIR-LMC35x: 2.13 in. (5.4 cm) x 3.31 in. (8.4 cm) x 0.1 in. (0.3 cm) AIR-PCI35x: 6.6 in. (16.8 cm) x 3.9 in. (9.8 cm) x .5 in. (1.3 cm)
Weight	AIR-PCM35x: 1.6 oz (45g) AIR-LMC35x: 1.4 oz (40g) AIR-PCI35x: 4.4 oz (125g)
Environmental	AIR-PCM35x and AIR-LMC35x: -22° to 158° F (-30° to 70° C) AIR-PCI35x: 32° to 131° F (0° to 55° C) 10 to 90% (noncondensing)
Input Power Requirements	+5 VDC =/- 5%
Typical Power Consumption (at 100 mW transmit power setting)	Transmit: 450 mA; Receive: 270 mA; Sleep mode: 15 mA

[1] Maximum power setting will vary according to individual country regulations.

Selected Part Numbers and Ordering Information[1]

Cisco Aironet 350 Series Client Adapters

AIR-PCM352	350 Series PC Card with Diversity Antennas & 128-bit WEP
AIR-PCI352	350 Series PCI Card with 2.2 dBi Dipole Antenna & 128-bit WEP

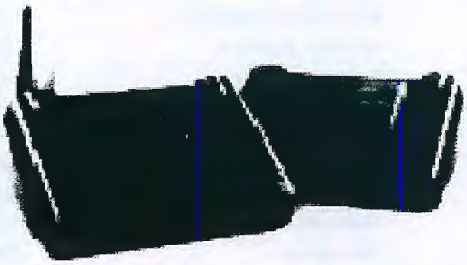
[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability)

4703 E

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 350 Series Workgroup Bridge



Designed to meet the needs of remote workgroups, satellite offices, and mobile users, the Cisco Aironet 350 Series Workgroup Bridge brings the freedom and flexibility of wireless connectivity to any Ethernet-enabled device. The 802.11b workgroup bridge quickly connects up to eight Ethernet-enabled laptops or other portable computers to a wireless LAN (WLAN), providing a link from these devices to any Cisco Aironet Access Point (AP) or Wireless Bridge (line-of-sight).

Any Ethernet-ready device, including printers, copiers, PCs, point-of-sale devices, or monitoring equipment, can be placed directly at the point of work using the workgroup bridge—without the expense or delay of cabling. For temporary classrooms or temporary office space, the workgroup bridge provides flexible, easy network access for up to eight devices through the use of a standard eight-port Ethernet hub. Equipment can be easily moved as workgroups change in number or location, lowering facilities costs.

The Cisco Aironet 350 Series Workgroup Bridge supports Wired Equivalent Privacy (WEP) security architecture and provides up to 128-bit encryption. The Cisco Aironet security architecture is based upon an IEEE 802.11x standard utilizing the Extensible Authentication Protocol (EAP), an open standard that enables wireless manufacturers and RADIUS server vendors to independently develop interoperable hardware and software. For authentication of devices attached to the workgroup, a username and password may be stored in the workgroup bridge in either static or dynamic memory. When authenticated, the workgroup bridge receives a single-session, single-user encryption key from the Remote Access Dial-In User Service (RADIUS) server via the associated AP. With this centralized and standards-based architecture, wireless security scales to meet the requirements of any enterprise.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 350 Series Workgroup Bridge	• Connectivity to a network for remote workgroups located in an area that may be difficult or not practical for wiring. • Supports up to eight Ethernet-based devices (with use of Ethernet hub)

Key Features

- Driverless installation of up to eight Ethernet-enabled devices
- Optimum wireless performance and range
- Standards-based centralized security
- Two versions for a range of application requirements
- Full-featured utilities and robust management

Specifications

Feature	Cisco Aironet 350 Series Workgroup Bridge
Data Rates Supported	1, 2, 5.5, and 11 Mbps
Client Interface	10BaseT Ethernet
Clients Supported	Direct: One Via hub: Eight
Network Architecture Types	Infrastructure (via Cisco Aironet Access Point or Bridge)
Frequency Band	2.4 to 2.4897 GHz
Wireless Medium	Direct Sequence Spread Spectrum (DSSS)
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	DBPSK @1 Mbps; DQPSK @ 2 Mbps; CCK @ 5.5 and 11 Mbps
Operating Channels	North America: 11; ETSI: 13; Japan: 14
Nonoverlapping Channels	Three
Receive Sensitivity	1 Mbps: -94 dBm; 2 Mbps: -91 dBm; 5.5 Mbps: -89 dBm; 11 Mbps: -85 dBm
Delay Spread	1 Mbps: 500 ns; 2 Mbps: 400 ns; 5.5 Mbps: 300 ns; 11 Mbps: 140 ns
Available Transmit Power Settings[1]	100 mW (20 dBm); 50 mW (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm)
Range (typical)	Indoor: 130 ft (40 m) @ 11 Mbps; 350 ft (107 m) @ 1 Mbps Outdoor: 800 ft (244 m) @ 11 Mbps; 2000 ft (610 m) @ 1 Mbps
Compliance	Operates license free under FCC Part 15 and complies as a Class B device; complies with DOC regulations; complies with EN 300.328 standards
SNMP Compliance	MIB I and MIB II
Antenna	AIR-WGB352C: One nonremovable 2.2-dBi dipole AIR-WGB352R: Two RP-TNC connectors (antennas optional, none supplied with unit)
Encryption Key Length	AIR-WGB352x: 128-bit
Remote Configuration Support	Telnet, HTTP, FTP, TFTP, and SNMP
Dimensions (W x D x H)	6.30 in. (16 cm) x 4.72 in. (12 cm) x 1.45 in. (3.7 cm)
Weight	12.3 oz (350g)
Environmental	Temperature: 32° to 122° F (0° to 50° C); 10 to 90% (Noncondensing)
Input Power Requirements	North American: 120 VAC @ 60 Hz; Universal: 90 to 264 VAC @ 47 to 63 Hz

[1] Maximum power setting will vary according to individual country regulations.

Selected Part Numbers and Ordering Information[1]

Cisco Aironet 350 Series Workgroup Bridge

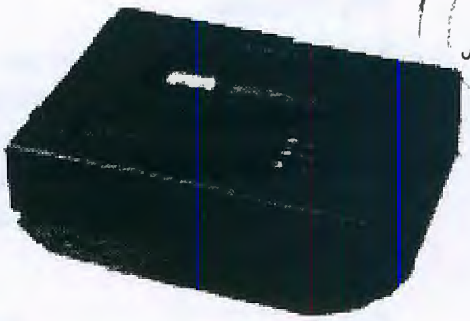
AIR-WGB352C	350 Series Workgroup Bridge with Captured Antenna & 128-bit WEP
AIR-WGB352R	350 Series Workgroup Bridge with Dual RP-TNC & 128-bit WEP

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability)

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet 350 Series Wireless Bridge



The Cisco Aironet 350 Series Wireless Bridge enables high-speed long-range outdoor links between buildings and is ideal for installations subject to plenum rating and harsh environments. It is designed to meet the requirements of even the most challenging applications. The 802.11b wireless bridge delivers high data rates and superior throughput for data-intensive, line-of-sight applications. The bridges connect hard-to-wire sites, noncontiguous floors, satellite offices, school or corporate campus settings, temporary networks, and warehouses. They can be configured for point-to-point or point-to-multipoint applications and allow multiple sites to share a single, high-speed connection to the Internet. For functional flexibility, the wireless bridge may also be configured as an access point.

The Cisco Aironet 350 Series Wireless Bridge features an extended operating temperature range of -20° to 55° C, allowing for placement outdoors in a NEMA enclosure or in harsh indoor environments such as warehouses and factories. With a durable metal case, the Cisco Aironet 350 Series Wireless Bridge is UL 2043 certified, and designed to achieve plenum rating as defined by various municipal fire codes.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Aironet 350 Series Ethernet Bridge	• Any company who needs to connect sites into a single LAN, even when separated by obstacles such as freeways, railroads and bodies of water that are normally inaccessible via cabling. • Business owners who want a low-cost, easy-to-deploy solution for connecting line-of-sight networks located in different buildings. • Business owners or IT directors who want multiple buildings on a campus to share a single high-speed line to the Internet.

Key Features

- High-speed (11-Mbps), high-power (100-mW) radios, delivering building-to-building links of up to 25 miles (40.2 km)
- A metal case for durability and plenum rating and an extended operating temperature rating for harsh environments
- Supports both point-to-point and point-to-multipoint configurations
- Broad range of supported antennas
- Simplified installation, improved performance, and upgradeable firmware, ensuring investment protection

Specifications

Feature	Cisco Aironet 350 Series Wireless Bridge
Data Rates Supported	1, 2, 5.5, and 11 Mbps
Frequency Band	2.4 to 2.497 GHz
Wireless Medium	Direct Sequence Spread Spectrum (DSSS)
Media Access Protocol	Carrier sense multiple access with collision avoidance (CSMA/CA)
Modulation	DBPSK @1 Mbps DQPSK @ 2 Mbps CCK @ 5.5 and 11 Mbps
Operating Channels	North America: 11; ETSI: 13; Japan: 14
Nonoverlapping Channels	Three
Receive Sensitivity	1 Mbps: -94 dBm; 2 Mbps: -91 dBm; 5.5 Mbps: -89 dBm; 11 Mbps: -85 dBm
Delay Spread	1 Mbps: 500 ns; 2 Mbps: 400 ns; 5.5 Mbps: 300 ns; 11 Mbps: 140 ns
Available Transmit Power Settings[1]	100 mW (20 dBm); 50 mW (17 dBm); 30 mW (15 dBm); 20 mW (13 dBm); 5 mW (7 dBm); 1 mW (0 dBm)
Range (typical, contingent upon antenna selected)	18 miles (28.9 km) @ 11 Mbps Up to 25 miles (40.2 km) @ 2 Mbps
Compliance	Operates license-free under FCC Part 15 and complies as a Class B device; complies with DOC regulations; complies with ETS 300.328, FTZ 2100, and MPT 1349 standards; complies with UL 2043 (The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local industry Canada office.)
SNMP Compliance	MIB I and MIB II
Antenna	Two RP-TNC connectors (antennas optional, none supplied with unit)
Encryption Key Length	128-bit
Security	128-bit WEP in bridge mode IEEE 802.11x (includes EAP and RADIUS) in AP mode
Status Indicators	Three indicators on the top panel provide information concerning association status, operation, error/warning, firmware upgrade, and configuration, network/modem, and radio status
Automatic Configuration Support	BOOTP and DHCP
Remote Configuration Support	Telnet, HTTP, FTP, TFTP, and SNMP
Local Configuration	Direct console port (with supplied serial cable)
Bridging Protocol	Spanning Tree
Dimensions	6.74 x 6.25 x 1.31 in. (17.1 x 15.9 x 3.3 cm)
Weight	1.43 lbs (.648 kg)
Environmental	Temperature: -4× to 131× F (-20× to 55× C) 10 to 90% (noncondensing)
Enclosure	Metal case (for plenum rating); UL 2043 certified
Input Power Requirements	24VDC 10% to 60 VDC (Ethernet line power)

[1] Maximum power setting will vary according to individual country regulations

Selected Part Numbers and Ordering Information[1]

Cisco Aironet 350 Series Wireless Bridge

AIR-BR350-x-K9	350 Series 11Mbps DSSS Bridge with 128-bit WEP

Cisco Aironet 350 Series Wireless Bridge Basic Maintenance

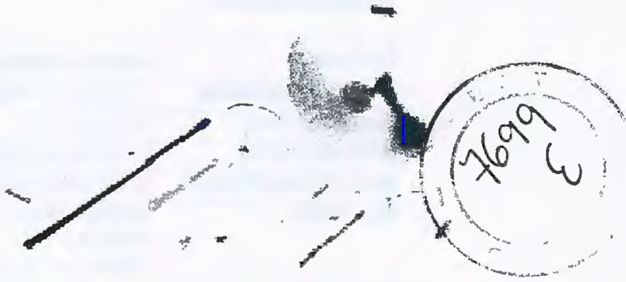
CON-SNT-PKG2	SMARTnet Maintenance for AIR-BR350-A-K9

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Aironet Web site: **http://www.cisco.com/go/aironet**

Cisco Aironet Antennas and Accessories



7699 3

Every wireless Local Area Network (LAN) deployment is different. When engineering an in-building solution, varying facility sizes, construction materials, and interior divisions raise a host of transmission and multipath considerations. When implementing a building-to-building solution, distance, physical obstructions between facilities, and number of transmission points involved must be considered.

Cisco is committed to providing not only the best access points, client adapters, and bridges in the industry—it is also committed to providing a complete solution for any wireless LAN deployment. That is why Cisco has the widest range of antennas, cable, and accessories available from any wireless manufacturer.

With the Cisco FCC-approved directional and omnidirectional antennas, low-loss cable, mounting hardware, and other accessories, installers can customize a wireless solution that meets the requirements of even the most challenging applications.

Key Features

- Client Adapter Antennas—Cisco Aironet wireless client adapters come complete with standard antennas that provide sufficient range for most applications at 11 Mbps. To extend the transmission range for more specialized applications, a variety of optional, higher-gain antennas are provided that are compatible with selected client adapters
- Access Point Antennas—Cisco Aironet access point antennas are compatible with all Cisco RP-TNC-equipped access points. The antennas are available with different gain and range capabilities, beam widths, and form factors. Coupling the right antenna with the right access point allows for efficient coverage in any facility, as well as better reliability at higher data rates
- Bridge Antennas—Cisco Aironet bridge antennas allow for extraordinary transmission distances between two or more buildings. Available in directional configurations for point-to-point transmission and omnidirectional configuration for point-to-multipoint implementations, Cisco has a bridge antenna for every application
- Low-loss cable extends the length between any Cisco Aironet bridge and the antenna. With a loss of 6.7 dB per 100 feet (30m), low-loss cable provides installation flexibility without a significant sacrifice in range

Specifications

Client Adapter Antennas

Feature	AIR-ANT3351
Description	POS diversity dipole[1]
Application	Indoor diversity antenna[2] to extend the range of Aironet LMC client adapters
Approximate Indoor Range at 1 Mbps[3]	350 ft (107m)
Approximate Indoor Range at 11 Mbps[3]	100 ft. (51 m)
Cable Length	5 ft. (1.5m)
Dimensions	Base: 7 x 2 in. (18 x 5 cm) Height: 8 in. (20 cm)
Weight	9.2 oz. (261g)

[1] A type of low-gain (2.2 dBi) antenna consisting of two (often internal) elements.

[2] A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain and, as such, the more acute the angle of coverage.

[3] All range estimations are based on an integrated client adapter antenna associating with an access point under ideal indoor conditions. The distances referenced here are approximations and should be used for estimation only.

Access Point Antennas

Feature	AIR-ANT5959	AIR-ANT3195	AIR-ANT2012	AIR-ANT3213
Description	Diversity omni-directional ceiling mount	3 dBi Patch Wall Mount Antenna	Diversity patch wall mount	Pillar mount diversity omni
Application	Indoor unobtrusive antenna, best for ceiling mount. Excellent throughput and coverage solution in high multipath cells and dense.	Indoor/Outdoor directional antenna	Indoor/Outdoor, unobtrusive medium range antenna	Indoor, unobtrusive medium-range antenna
Approximate Indoor Range at 1 Mbps[1]	350 ft. (105m)	Access Point: 271 ft. (82m) Bridge: .5 miles (.9 km)	547 ft. (167m)	497 ft. (151m)
Approximate Indoor Range at 11 Mbps[1]	130 ft. (45m)	Access Point: 80 ft. (24m) Bridge: 950 ft. (290m)	167 ft. (51m)	142 ft. (44m)
Cable Length	3 ft. (0.91m)	12 ft.	3 ft. (0.91m)	3 ft. (0.91m)
Dimensions	5.3 x 2.8 x 09. in. (13.5 x 7.1 x 2.3 cm)	4 x 5 in. (9.7 x 13 cm)	4.78 x 6.66 x .82 in. (12.14 x 16.92 x 2.08 cm)	10 x 1 in. (25.4 x 2.5 cm)
Weight	0.3 lbs. (0.14kg)	4.9 oz. (139g)	9.6 oz. (272g)	1 lb. (460g)

[1] All range estimations are based on an integrated client adapter antenna associating with an access point under ideal indoor conditions. The distances referenced here are approximations and should be used for estimation only.

Access Point Antennas (cont.)

Feature	AIR-ANT1728	AIR-ANT4941	AIR-ANT3549	AIR-ANT1729
Description	High gain omnidirectional ceiling mount	2.2 dBi dipole antenna	Patch wall mount	Patch wall mount
Application	Indoor medium-range antenna, typically hung from crossbars of drop ceilings	Indoor omni-directional coverage	Indoor, unobtrusive, long-range antenna (may also be used as a medium-range bridge antenna)	Indoor, unobtrusive, medium-range antenna (may also be used as a medium-range bridge antenna)
Approximate Indoor Range at 1 Mbps[1]	497 ft. (151m)	350 ft.	Access Point: 700 ft. (213m) Bridge: 2.0 miles (3.2 km)	Access Point: 542 ft. (165m) Bridge: 1.1 miles (1.8 km)
Approximate Indoor Range at 11 Mbps[1]	142 ft. (44m)	130 ft.	Access Point: 200 ft. (61m) Bridge: 3390 ft. (1032m)	Access Point: 155 ft. (47m) Bridge: 1900 ft. (580m)
Cable Length	3 ft. (0.91m)	N/A	3 ft. (0.91m)	3 ft. (0.91m)
Dimensions	Length: 9 in. (22.86 cm) Diameter: 1 in. (2.5 cm)	5.5 in.	5 x 5 in. (12.4 x 12.4 cm)	4 x 5 in. (9.7 x 13 cm)
Weight	4.6 oz. (131g)	1.1 oz.	5.3 oz. (150g)	4.9 oz. (139g)

[1] All range estimations are based on an integrated client adapter antenna associating with an access point under ideal indoor conditions. The distances referenced here are approximations and should be used for estimation only.

Bridge Antennas

Feature	AIR-ANT2506	AIR-ANT4121	AIR-ANT1949	AIR-ANT3338
Description	Omnidirectional Mast mount	High-gain omnidirectional Mast mount	Yagi mast mount	Solid dish
Application	Outdoor short-range point-to-multipoint applications	Outdoor medium-range point-to-multipoint applications	Outdoor medium-range directional connections	Outdoor long-range directional connections
Approximate Indoor Range at 1 Mbps[1]	5000 ft. (1525m)	4.6 miles (7.4 km)	6.5 miles (10.5 km)	25 miles (40 km)
Approximate Indoor Range at 11 Mbps[1]	1580 ft. (480m)	1.4 miles (2.3 km)	2.0 miles (3.3 km)	11.5 miles (18.5 km)
Cable Length	3 ft. (0.91m)	1 ft. (0.30m)	1.5 ft. (0.46m)	2 ft. (0.61m)
Dimensions	Length: 13 in. (33 cm) Diameter: 1 in. (2.5 cm)	Length: 40 in. (101 cm) Diameter: 1.3 in. (3 cm)	Length: 18 in. (46 cm) Diameter: 3 in. (7.6 cm)	Diameter 24 in. (61 cm)
Weight	6 oz. (17g)	1.5 lb. (0.68 kg)	1.5 lb. (0.68 kg)	11 lb. (5 kg)

[1] All range estimations are based on an integrated client adapter antenna associating with an access point under ideal indoor conditions. The distances referenced here are approximations and should be used for estimation only.

Low-Loss/Ultra Low-Loss Antenna Cable

Feature	AIR-CAB020LL-R	AIR-CAB050LL-R	AIR-CAB100ULL-R	AIR-CAB150ULL-R
Cable Length	20 ft. (6m)	50 ft. (15m)	100 ft. (30m)	150 ft. (46m)
Transmission Loss	1.3 dB	3.4 dB	4.4 dB	6.6 dB

Cisco Aironet Accessories

Feature	AIR-ACC2537-060	AIR-ACC3354	AIR-ACC2662
Description	60 in. (152 cm) bulkhead extender	Lightning arrestor	Yagi articulating mount
Application	Flexible antenna cable that extends access point cabling typically within an enclosure	Helps prevent damage due to lightning-induced surges or static electricity	Adds swiveling capability to mast-mounted yagi antennas

Selected Part Numbers and Ordering Information[1]

Cisco Aironet Accessories	
AIR-ACC2662	Yagi Antenna Articulating Mount
AIR-ACC3354	Lightning Arrestor w/ grounding ring
AIR-CAB020LL-R	20 ft. (6m) low-loss antenna cable
AIR-CAB050LL-R	50 ft. (15m) low loss antenna cable
AIR-CAB100ULL-R	100 ft. (30m) low loss antenna cable
AIR-CAB150ULL-R	150 ft. (46m) low loss antenna cable
Cisco Aironet Antennas	
AIR-ANT1728	5.2 dBi Omni Ceiling Mount Antenna
AIR-ANT1729	6 dBi Patch Wall Mount Antenna
AIR-ANT1949	13.5 dBi Yagi Mast Mount Antenna
AIR-ANT2012	6.5 dBi Diversity Patch Wall Mount Antenna
AIR-ANT2506	5.2 dBi Omnidirectional Mast Mount Antenna
AIR-ANT3195	3 dBi Patch Wall Mount Antenna
AIR-ANT3213	5.2 dBi Pillar-Mount Diversity Omni Antenna
AIR-ANT3338	21 dBi Solid Dish Antenna
AIR-ANT3351	2.2 dBi POS Diversity Dipole Antenna
AIR-ANT3549	8.5 dBi Hemispherical Patch Antenna
AIR-ANT4121	12 dBi Omnidirectional Mast Mount Antenna
AIR-ANT4941	2.2 dBi Dipole Antenna (Standard Rubber Duck)
AIR-ANT5959	2.0dBi Diversity Omni Ceiling Mount Antenna

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Aironet Antennas & Accessories Web site **http://www.cisco.com/go/antenna**

CHAPTER 4

IP Telephony, Video, & Web Collaboration

Campus IP Telephony, Video, & Web Collaboration at a Glance

Product	Features	Page
Cisco IP Phones IP 7900 Series	An exciting, distinctively stylish, and pure Voice over IP phone portfolio to meet the wide range of business communication needs at affordable prices • Display-based technology provides ease-of-use • Integrated inline power and 2-port Ethernet Switch provides end-to-end infrastructure integration • Rich application environment enabled by open APIs based on XML	4-3
Cisco CallManager 3.3	• The software-based call processing and call control component of Cisco's IP Telephony solution • Resides on Cisco Media Convergence Servers (MCS), Cisco ICS7750, or selected third-party servers (CallManager 3.3)	4-4
CiscoWorks IP Telephony Environment Monitor	A suite of management applications that helps ensure the readiness and manageability of converged networks that are supporting VoIP and IP telephony traffic and applications. The bundle includes: • Voice Health Monitor • Default Fault Manager • CiscoView • CCO Downloadable Modules: – IP Phone Information Utility – IP Phone Help Desk Utility. – Fault History Manager	9-18
Cisco IP Contact Center (IPCC) Enterprise Edition	Cisco IP Contact Center (IPCC) Enterprise Edition delivers intelligent call routing, network-to-desktop CTI, and multi-channelmedia contact management to contact center agents over an IP network. It includes several applications, including the following: • CallManager • Cisco Intelligent Contact Manager (ICM) • Cisco IP IVR/-IP Queue Manager	4-8
Cisco IP IVR	Cisco IP IVR, a new world interactive voice response (IVR) solution, provides a feature-rich foundation for the creation of an IP-based IVR that is open and expandable. Cisco IP IVR has the following key features: • Provides a multimedia (voice/data/Web) IP-empowered application-generation environment • Can be deployed anywhere in the IP network • Offers Web-based activation and administration	4-10
Cisco IP Contact Center Express Edition (Formerly IP ICD)	• Cisco IPCC Express is a software-based ACD, IVR, and CTI application for mid-sized contact centers with Cisco IP Telephony networks based on Cisco AVVID. • Cisco IPCC Express is an open systems platform allowing ease of configuration. • It has a graphically driven workflow editor providing a common interface for creating interactions, or call flows, and creates business logic between IVR and ACD functions.	4-9
Cisco Unity—Unified Messaging and Voice Mail	Voicemail and unified messaging system delivers all messages into single inbox for access via phone, email or Internet	4-11
Cisco Personal Assistant	Software application allows users to browse voicemail, dial by name, and conference from any phone using voice commands instead of telephone keypad via speech recognition	4-13
IP Telephony Applications	• Cisco Survivable Remote Site (SRS) Telephony Software—IOS software that runs on local branch office router provides IP Telephony backup redundancy for IP phones in that office when IP phones detect that WAN is down or/and CallManager is unreachable • Cisco IP Phone Messenger—sends Instant Messages (IM) between Cisco IP Phones and Lotus Sametime or MS Messenger desktop IM clients • Cisco IP SoftPhone—Windows-based application for PC, allows users to make and receive calls from PC without a dedicated phone • Cisco Conference Connection (CCC)—enables enterprises to bring geographically dispersed employees and customers together to facilitate meetings and collaboration. CCC provides a cost-effective and time-efficient method of doing business without the hassle of travel.	4-14

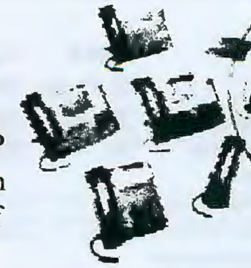
7695 3

Product	Features	Page
Cisco MCS 7800 Series Media Convergence Servers	High availability server platform for Cisco IP telephony systems • Turnkey solution, includes CallManager or other software • For large- and medium-sized enterprise IP telephony deployments	4-17
Cisco ICS 7750 Integrated Communications System	• A branch office/midmarket business with standalone IP telephony needs from 35-500 users • An end-user customer or partner who wants a single "box" (or platform) IP telephony solution to ease deployment and/or to standardize on voice configurations across multiple sites • An existing multiservice data network customer who wants to add IP telephony functionality to create a converged network solution	4-18
Cisco IAD 2400 Series Integrated Access Device[1]	Business class fixed-configuration Integrated Access Device (IAD) • Delivers packet or TDM voice and data over single WAN uplink • IOS Telephony Service (ITS) provides local IAD-based call processing to offer key switch functionality, ideal for small offices (5-24 phones) • IP-based keyswitch functionality, ideal for small offices (5-20 phones) who do not need Cisco CallManager capabilities • Supports standard phones and IP phones on a single platform • 8 FXS/16 FXS/16FXS+8FXO analog voice ports and 1 T1 digital voice port models • WAN Interfaces: T1- PPP, FR, ATM and DSL-ADSL and G.SHDSL	4-18
Cisco Voice Gateways[2]	The Cisco VG248 dedicated voice gateway provides connectivity between IP networks and legacy telephony systems/PSTN • Support various types of interfaces, including T1 and E1 • Fully manageable by Cisco CallManager, a CLI interface via Telnet, or via SNMP	4-22
Cisco IP/VC 3500 Series Videoconferencing Products	• Videoconferencing over IP solution • Cost-effective, easy-to-manage • Translates between H.323 and H.320 systems • Management and Quality of Service	4-22
Cisco IP/TV 3400 Series Video Servers	• High-quality video communications over enterprise networks • Support live and scheduled video, video on demand • Enable training, corporate communications, business TV, and distance learning	4-23
Cisco Web Collaboration Option	• Web-based collaboration, • Share any Windows desktop application • Ideal for both sales- and service-oriented customer service organizations	4-24
Cisco E-mail Manager	• Automates the process of tracking and responding to inbound email. • Automatically assigns email requests to the most appropriate agent • Graphical rules engine makes it easy to define custom rules for the processing of email	4-25
Cisco Emergency Responder	• Works with Cisco CallManager to automatically provide E9-1-1 features in North America, and is compatible with any emergency number including 112 in Europe, 999 in UK, and 000 in Australia. • Dynamically tracks the location of IP phones, routes emergency calls to the appropriate E9-1-1 network, and provides the current location information to E9-1-1 call center dispatchers. • Provides real-time alert notifications to on-site or contracted security groups, to facilitate a timely response to emergency situations.	4-25
Cisco ATA Series of Analog Telephone Adaptors	Turns any analog telephone into an IP telephone. Each of the two voice ports supports independent telephone numbers, providing two separate lines. • Interoperable with multiple standards including H.323, SIP, MGCP and SCCP • Enables analog devices, such as phones and fax machines, to support Voice over IP services by converting the analog signal into an IP signal	4-27
Cisco CTE-1400 Series Content Transformation Engine	Transforms Web content for display and interaction on small screen mobile devices and IP Telephones • Supports a broad range of devices • Transforms existing content • GUI/Console Administrative Tool	6-13

[1] IP Keyswitch capabilities also available with 2600/2600XM and 3600 series routers; see IP Keyswitch Web site: http://www.cisco.com/go/keyswitch

[2] Cisco's full line of multiservice routers also provide analog and digital voice gateway functionality through use of network modules and voice interface cards. Please see the 1700, 2600XM, 3600, 7200, 5x00 series in Chapter 1—Routers, as well as Chapter 7—Access Products.

Cisco 7900 Series IP Phones



Cisco IP Phones provide unmatched levels of integrated business functionality and converged communications beyond today's conventional voice systems. The Cisco IP Phone7960G "manager set" addresses the communication needs of the professional, with a high or busy amount of phone traffic. The Cisco IP Phone 7940G "business set" addresses the communication needs of a transaction type worker, in a office cubicle environment, who conducts medium to high telephone traffic. The Cisco IP Phone 7912G, 7910G+SW, 7910G, and 7905G "basic sets" address the communication needs of a cubicle worker who conducts low to medium telephone traffic. The Cisco IP Phone 7902G "entry set" addresses voice communication needs of a lobby, lab, manufacturing floor, and other areas where only a minimal amount of features are required. Cisco IP Phone Expansion Module 7914 extends the Cisco IP Phone 7960G with additional buttons and LCD, increasing the total number of buttons to 20 with one module, or 34 with two modules. Cisco IP Conference Station 7935, a high-quality hands-free conference station, is designed for use on desktops and offices and in small to medium-sized conference rooms.

Key Features

- Dynamic soft keys make the telephone simpler to use by presenting calling options based on context
- Open APIs using XML to deliver applications to the display
- Automatic phone discovery, VLAN configuration, and registration
- Quality of Service (QoS) is provided via support of 802.1pq, in addition to configurable DIFFSERV and TOS
- Voice-activity detection, silence suppression, comfort-noise generation, and error concealment
- G.711a, G.711u, G.729ab audio-compression coder-decoders (codecs)
- Software upgrade support via Trivial File Transfer Protocol (TFTP) server
- Microsoft NetMeeting enabled—features such as application sharing and video conferencing are available simply by pressing a button on your Cisco IP telephone
- Integrated Ethernet Switch supporting Ethernet connectivity for a downstream PC
- Integrated Inline power support allows the phone to receive power over the LAN
- A hearing-aid-compatible handset

Specifications

Feature	Cisco IP Phone 7902G	Cisco IP Phone 7905G	Cisco IP Phone 7910G and 7910G+SW	Cisco IP Phone 7912G	Cisco IP Phone 7940G	Cisco IP Phone 7960G	Cisco 7914 Expansion Module	Cisco IP Conference Station 7935
Display	None	Pixel-Based	Character-Based	Pixel-based	Pixel-Based	Pixel-Based	Pixel-based	Character-Based
Dynamic Soft Keys	0	4	0	4	4	4	N/A	0
Inline Power	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
10/100Base-T Ethernet Switch	No	No	Yes, 7910G+SW No, 7910G	Yes	Yes	Yes	N/A	No
Lines	1	1	1	1	2	6	14	1

Feature	Cisco IP Phone 7902G	Cisco IP Phone 7905G	Cisco IP Phone 7910G and 7910G+SW	Cisco IP Phone 7912G	Cisco IP Phone 7940G	Cisco IP Phone 7960G	Cisco 7914 ExpansionModule	Cisco IP Conference Station 7935
Speaker Phone	No	Monitor Only	Monitor Only	Monitor Only	Yes	Yes	N/A	Yes
Headset Jack	No	No	No	No	Yes	Yes	N/A	No
3Rd Party XML Applications	No	No	No	No	Yes	Yes	N/A	No

Selected Part Numbers and Ordering Information[1]

Cisco 7900 Series IP Power and Phones

CP-7960G	Cisco IP Phone 7960G, Manager Set
CP-7940G	Cisco IP Phone 7940G, Business Set
CP-7912G	Cisco IP Phone 7912G, Basic Set w/ Switch
CP-7910G+SW	Cisco IP Phone 7910G+SW, Basic Set w/ Switch
CP-7910G	Cisco IP Phone 7910G, Basic Set
CP-7905G	Cisco IP Phone 7905G, Basic Set
CP-7902G	Cisco IP Phone 7902G, Entry Set
CP-7935	Cisco IP Conference Station
CP-7914=	Cisco 7914 IP Phone Expansion Module for the 7960 IP Phone
CP-SINGLFOOTSTAND=	Single module footstand
CP-DOUBLFOOTSTAND=	Double module footstand
CP-WALLMOUNTKIT=	Non-Locking Wall Mount Kit for 7910/40/60G series IP phones
CP-LCKNGWALLMOUNT=	Locking Wallmount Kit for the 7910/40/60G series IP phones
CP-PWR-CUBE=	IP Phone power transformer for 7900 series IP phones
WS-PWR-PANEL	Catalyst 48 port Inline Power Patch Panel

[1] This is only a small subset of all parts. Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco IP Telephones Web site: **http://www.cisco.com/go/iptel**

Cisco CallManager 3.3

Cisco CallManager call-processing software extends enterprise telephony features and capabilities to enterprise LANs and packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Additional data, voice, and video services such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems interact with the IP telephony solution through CallManager's open telephony application programming interfaces (API). Cisco CallManager is installed on the Cisco Media Convergence Server (MCS) and selected third-party servers. It ships with a suite of integrated voice applications and utilities, including the Cisco Attendant Console—a software-only manual attendant console; a conferencing application; and administrative reporting tools. For more VoIP network management features, see the CiscoWorks Manager IP Telephony Environment Monitor, page 9-18.

Cisco CallManager version 3.3 provides a scalable, distributable, and highly available enterprise IP telephony call-processing solution. Multiple servers are clustered and managed as a single entity; yielding scalability of up to 30,000 users per cluster. By interlinking multiple clusters, system capacity can be increased to as many as one million users in a 100-site system. Clustering aggregates the power of multiple, distributed Cisco CallManagers, enhancing the scalability and accessibility of the servers to phones, gateways, and applications. Triple call-processing server redundancy improves overall system availability.

The benefit of this distributed architecture is improved system availability and scalability. Call admission control ensures that voice quality of service (QoS) is maintained across constricted WAN links, and automatically diverts calls to alternative Public Switched Telephone Network (PSTN) routes when WAN bandwidth is not available. A Web-browsable interface to the configuration database enables remote device and system configuration.

Key Features

- Cisco CallManager includes a suite of integrated voice applications that perform voice conferencing and manual attendant console functions, eliminating the need for special-purpose voice processing hardware
- Supplementary and enhanced services such as hold, transfer, forward, conference, multiple line appearances, automatic route selection, speed dial, last-number redial, and other features are extended to IP phones and gateways
- Capabilities enhancements are achieved though software upgradeability, avoiding expensive hardware costs traditional to legacy PBX systems
- Cisco CallManager Attendant Console—This Web-enabled application supports the traditional role of a manual attendant console and allows the attendant to quickly accept and dispatch calls to enterprise users. An integrated directory service provides traditional busy lamp field (BLF) and direct station select (DSS) functions for any line in the system. It monitors the state of every line in the system without requiring hardware-based line monitoring devices, thereby saving costs
- Software-only applications such as the Cisco Interactive Voice Response system, Cisco IP Contact Center, Cisco Automated Attendant, and Cisco SoftPhone are applications that interact with the CallManager through telephony APIs

Specifications

Feature	Cisco CallManager 3.3[1]
Platforms	Media Convergence Server (MCS) Integrated Communications Server (ICS-7750) Selected third-party servers
Pre-Installed Software	Cisco CallManager version 3.3 (call processing and call-control application) Cisco CallManager version 3.3 configuration database (contains system and device configuration information, including dial plan) Cisco CallManager Administration software Cisco Conference Bridge Cisco Attendant Console Bulk Administration Tool (BAT) CDR Analysis and Reporting (CAR) tool Real Time Monitoring Tool RTMT
Sample Subset of System Capabilities	H.323 scalability improvements - 1,000 H.323 calls per CallManager server in cluster Virus checker certification Cisco Intrusion Detection System (IDS) Host-Based Sensor certification

Feature	Cisco CallManager 3.3[1]
Summary of Administrative Features	Application discovery and registration to SNMP manager
	Automated Alternate Routing Groups
	Bulk Administration
	Call Back
	Call Detail Records (CDR)
	Call forward reason code delivery
	Centralized, replicated configuration database, distributed Web-based management viewers
	Configurable and default ringer WAV files per phone
	Configuration database API
	Database automated change notification
	Date/time display format configurable per phone
	Debug information to common syslog file
	Device addition through wizards
	Device downloadable feature upgrades—Phones, hardware transcoder resource, hardware conference bridge resource, VoIP gateway resource
	Device groups and pools for large system management
	Device mapping tool-IP address to MAC address
	Distinctive ring per line
	Dynamic Host Configuration Protocol (DHCP) block IP assignment-phones and gateways
	Dialed number translation table (inbound/outbound translation)
	Dialed Number Identification Service (DNIS)
	Enhanced 911 service
	H.323-compliant interface to H.323 clients, gateways, and gatekeepers
	Individual line Call Waiting Alert Configuration
	JTAPI 1.2 computer telephony interface
	LDAP version 3 directory interface to selected vendor's LDAP directories • Active Directory • Netscape Directory Server
	Manager Assistant
	Mappable softkeys
	MGCP signaling and control to selected Cisco VoIP gateways
	Multilevel Administration Access (MLA)
	Native supplementary services support to Cisco H.323 gateways
	Network Specific Facilities Paperless phone DNIS-display driven button labels on phones
	Performance monitoring SNMP statistics from applications to SNMP manager or to operating system
	Performance Monitor
	QoS statistics recorded per call
	Q.SIG Support
	Redirected DNIS (RDNIS), inbound, outbound (to H.323 devices)
	Select specified line appearance to ring; Select specified phone to ring
	Single CDR per cluster
	Single point system/device configuration
	Sortable component inventory list by device, user, or line
	System event reporting-to common syslog or operating system event viewer
	TAPI 2.1 computer telephony interface
	Time-zone configurable per phone
	XML API into IP phones (794X/6X)
	Zero cost automated phone moves; Zero cost phone adds

Feature	Cisco CallManager 3.3[1]
Summary of User Features	Answer/answer release
	Auto-answer/[2]intercom
	Call connection
	Call coverage
	Call forward-all (off-net/on-net); Call forward-busy; Call forward-no answer
	Call hold/retrieve
	Call park/pickup; Call pickup group-universal
	Call status per line (state, duration, number)
	Call waiting/retrieve
	Calling Line Identification (CLID); Calling party name identification (CNID)
	Calling Line Identifiation Restriction (CLIR)
	Direct inward dial (DID; Direct outward dial (DOD)
	Directory dial from phone-corporate, [2]personal
	Directories-missed, placed, received calls list stored on selected IP phones
	Distinctive ring (on-net vs. off-net); Distinctive ring per phone
	Drop last conference party (ad-hoc conferences)
	Extension mobility support
	Hands-free, full-duplex speakerphone
	HTML help access from phone
	Last number redial (off-net/on-net)
	Message waiting indication
	Multiparty conference-Ad-hoc with add-on, Meet-me
	Multiple line appearances per phone
	Music-on-hold
	Mute capability from speakerphone and handset
	On-hook dialing
	Operator attendant-Web-browser interface, loop key notification, logon/logoff, busy/available, left/right hand access, headphone access, busy lamp field, direct station select, drag and drop transfer, call status (state, duration, and number)
	Privacy
	Real-time QoS statistics through http browse to phone
	Recent dial list-calls to phone, calls from phone, auto-dial, and edit dial
	Single button data collaboration on SoftPhone-chat, whiteboard, and app sharing
	Single directory number, multiple phones-bridged line appearances
	Speed dial-multiple speed dials per phone
	Station volume controls (audio, ringer)
	Transfer-with consultation hold
	User-configured speed dial and call forward through Web access
	Web services access from phone
	Wideband audio codec support—proprietary 16-bit resolution, 16 kHz sampling rate codec

1. Additional RAM may be required in Media Convergence Servers to support existing and enhanced services in Cisco CallManager 3.3.
2. Indicates new feature or service for Cisco CallManager version 3.3

For More Information

See the Cisco CallManager Web sites: **http://www.cisco.com/go/callmgr**

Selected Part Numbers and Ordering Information[1]

Cisco IP Integrated Contact Distribution (ICD)

ICD-3.0-STD-BS SW	Standard ICD 3.0 Standard Bundle
ICD-3.0-STD-BB	Bid Set ICD 3.0 Standard Bundle
ICD-3.X-S-AGT1	1 Cisco Standard Agent Desktop ICD 3.X
ICD-3.X-S-AGT5	5 Cisco Standard Agent Desktops ICD 3.X
ICD-3.X-S-AGT10	10 Cisco Standard Agent Desktops ICD 3.X
ICD-3.X-S-AGT25	25 Cisco Standard Agent Desktops ICD 3.X
ICD-3.X-S-AGT50	50 Cisco Standard Agent Desktops ICD 3.X
ICD-3.X-S-SUP1	1 Cisco Standard Supervisor Desktop ICD 3.X
ICD-3.X-S-HIST1	1 Cisco Standard Historical Reporting ICD 3.X
ICD-3.0-ENH-BS	ICD 3.0 Enhanced Bundle
ICD-3.X-E-AGT1	1 Cisco Enhanced Agent Desktop ICD 3.X
ICD-3.X-E-AGT5	5 Cisco Enhanced Agent Desktops ICD 3.X
ICD-3.X-E-AGT10	10 Cisco Enhanced Agent Desktops ICD 3.X
ICD-3.X-E-AGT25	25 Cisco Enhanced Agent Desktops ICD 3.X
ICD-3.X-E-AGT50	50 Cisco Enhanced Agent Desktops ICD 3.X
ICD-3.X-E-SUP1	1 Cisco Enhanced Supervisor Desktop ICD 3.X
ICD-3.X-E-HIST1	1 Cisco Enhanced Historical Reporting ICD 3.X

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco IP Integrated Contact Distribution Web site:
http://www.cisco.com/go/icd

Cisco IP IVR

Cisco IP IVR, an interactive voice response (IVR) solution, provides a feature rich foundation for the creation of an IP-based Cisco IP IVR that is open and expandable. Written in Java to provide customer flexibility, IVR includes the following features:

- Multimedia (voice/data/Web) IP-empowered application-generation environment
- Support for optional Automated Speech Recognition (ASR) and Text-to-Speech (TTS)
- Support for VoiceXML
- Multiple Language support
- Cisco IP IVR can be located in anywhere the IP network
- Offers web-based activation and administration
- Flows (the IP IVR applications) are stored in an industry standard LDAP directory
- Cisco IP IVR is sold with Cisco CallManager and can be co-resident on the same server as CallManager or can function on a separate, dedicated media convergence servers (MCSs) or Cisco-approved customer provided server
- Packages available to scale up to 60 ports
- Cisco IP IVR offers enhanced scalability

Cisco Unity—Unified Messaging and Voice Mail

Cisco Unity is a powerful Unified Communications server that provides advanced, convergence-based communication services and integrates them with the desktop applications business professionals use everyday, improving customer service and productivity. Designed for enterprise-scale organizations, Cisco Unity delivers unified messaging that gives subscribers the ability to access and manage messages and calls from anywhere, at any time, regardless of device or media type. Subscribers can listen to e-mail over the telephone, check voice messages from the Internet, and if a fax server is present, forward faxes to any local fax machine. Cisco Unity voice messaging features robust automated attendant functionality that includes intelligent routing, and easily customizable call screening and message notification options. Cisco Unity supports localized versions in multiple languages and supports multiple languages on a single system.

Cisco Unity's optional digital networking module enables connectivity to other Cisco Unity servers at the same site via the LAN or remotely via WAN. Digital networking gives users the ability to send subscriber-to-subscriber messages anywhere in the world.

Cisco Unity supports both Cisco CallManager and leading legacy telephone systems—even simultaneously—to help smooth the transition to IP telephony and protect existing infrastructure investments. Built on a scalable platform, it uses streaming media and an intuitive HTML browser-style system administration interface. Costs are minimized when Cisco Unity's server architecture is truly unified with an organization's data network.

Key Features

- Architecture allows IT staff to set one back-up procedure, one message storage policy, and one security policy
- Enhanced scalability allows up to 72 ports per server; up to 7,500 subscribers per server; or a total of 250,000 users in an Exchange environment or 100,000 users in a Domino environment
- Support for Exchange 2000/Active Directory as the single message store and directory; AMIS-A and VPIM interoperability for Exchange systems
- Enhanced networking for large deployments—support for complex TDM telephone networks (multiple dialing domains)
- Support for multiple CCM clusters; ability to light Message Waiting Indicators
- With Exchange/Domino off-line, utilizes pre-MTA queue to take messages and give basic message access; Support for Lotus Domino as the single message store
- Fault-tolerant system tools—robust security, file replication, event logging, and optional software RAID levels 0-5
- Support for Windows 2000[1] in a mixed/native mode
- Unity Inbox/VMI (Visual Messaging Interface) is an Internet Explorer-based voice mail inbox providing unified messaging
- Unity Bridge provides advanced message interchange functionality with legacy Avaya/Octel voice mail systems—unlocking proprietary networking to deliver open standards-based IP migration

[1] Unity will not support Windows NT on the Unity server, although it can be installed into an NT environment.

Specifications

Feature	Cisco Unity 3.1
Unity Voice Mail (VM) and Unified Messaging (UM) Possible Configurations	16, 32 and Max sessions Configured for CallManager or configured for legacy PBX/dual integration[1]
Options	Voice Mail; Voice Mail with Multi-lingual option; Unified Messaging with Text-to-Speech (TTS) option Unified Messaging with Multi-lingual option; Exchange or Domino; AMIS for Exchange; VPIM for Exchange; Unity Inbox/Visual Messaging Interface; Failover for Exchange; Unity Bridge for Exchange

[1] Contact your Cisco Software Sales Representative for integration information.

7685
3

Selected Part Numbers and Ordering Information[1]

Cisco Unity Servers	
UNITY-SVR1400-1A	Dell 1400; rack-mountable; (W2K included)
UNITY-SVR2500A-1A	Dell 2500; rack-mount; 512MB; RAID 1 (W2K included)
UNITY-SVR2500C-2A	Dell 2500; rack-mount; 1GB; RAID 5, 2nd CPU, Win2K
UNITY-SVRX232-1A	IBM x232 rack; 512MB; RAID 1 (W2K included)
UNITY-SVRX232-2A	IBM x232 rack; 1GB; RAID 5, 2nd CPU (W2K included)
UNITY-SVRL570-1A	Compaq ML570 rack; 2GB; RAID 1(x2), RAID 5, Dual CPU, Win2K
UNITY-SVRL570-2A	Compaq ML570 rack; 4GB; RAID 1(x2), RAID 5, Quad CPU, Win2K
UNITY-SVR7827-1A	MCS 7827 rack:(W2K included)
UNITY-SVR7837-1A	MCS 7837 rack; 512MB; RAID 1 (W2K included)
UNITY-SVR7847-2A	MCS 7847 rack; 1GB; RAID 5, 2nd CPU (W2K included)
UNITY-EXP-CHAS=	Expansion chassis
Cisco Unity 3.1 Unified Messaging and Voicemail Software	
UNITYU50-4-3.1=	Unity Unified Messaging, 50 users (includes 4 sessions)
UNITYU100-8-3.1=	Unity Unified Messaging, 100 users (includes 8 sessions)
UNITYU200-12-3.1=	Unity Unified Messaging, 200 users (includes 12 sessions)
UNITYU300-16-3.1=	Unity Unified Messaging, 300 users (includes 16 sessions)
UNITYU500-24-3.1=	Unity Unified Messaging, 500 users (includes 24 sessions)
UNITYU875-32-3.1=	Unity Unified Messaging, 875 users (includes 32 sessions)
UNITYU1175-40-3.1=	Unity Unified Messaging, 1175 users (includes 40 sessions)
UNITYU1600-48-3.1=	Unity Unified Messaging, 1600 users (includes 48 sessions)
UNITYU2200-60-3.1=	Unity Unified Messaging, 2200 users (includes 60 sessions)
UNITYU2950-72-3.1=	Unity Unified Messaging, 2950 users (includes 72 sessions)
UNITYV50-4-3.1=	Unity Voice Messaging, 50 users (includes 4 sessions)
UNITYV100-8-3.1=	Unity Voice Messaging, 100 users (includes 8 sessions)
UNITYV200-12-3.1=	Unity Voice Messaging, 200 users (includes 12 sessions)
UNITYV300-16-3.1=	Unity Voice Messaging, 300 users (includes 16 sessions)
UNITYV500-24-3.1=	Unity Voice Messaging, 500 users (includes 24 sessions)
UNITYV875-32-3.1=	Unity Voice Messaging, 875 users (includes 32 sessions)
UNITYV1175-40-3.1=	Unity Voice Messaging, 1175 users (includes 40 sessions)
UNITYV1600-48-3.1=	Unity Voice Messaging, 1600 users (includes 48 sessions)
UNITYV2200-60-3.1=	Unity Voice Messaging, 2200 users (includes 60 sessions)
UNITYV2950-72-3.1=	Unity Voice Messaging, 2950 users (includes 72 sessions)
Cisco Unity Languages and Real Speak TTS	
UNITY-RS-2ML=	Unity, 2-port Real Speak TTS, US Eng, UK, Fr, Ger, Euro Sp
UNITY-RS-4ML=	Unity, 4-port Real Speak TTS. US Eng, UK, Fr, Ger, Euro Sp
UNITY-RS-6ML=	Unity, 6-port Real Speak TTS. US Eng, UK, Fr, Ger, Euro Sp
UNITY-MULTILANG=	Multiple Language support
UNITY-TWOLANG=	Add support for a second language
UNITY-AMIS=	Unity, AMIS-A networking

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco Unity site: **http://www.cisco.com/go/unity**

Cisco Personal Assistant

Cisco Personal Assistant streamlines communications with personal call rules, speech recognition, and productivity services for IP phones. As an integral part of Cisco AVVID (Architecture for Voice, Video and Integrated Data), it interoperates with Cisco CallManager and scales to meet the present and future needs of your employees. Users can access voice mail, dial by name, and conference from any telephone using speech recognition instead of the telephone keypad. The Web-based and telephone user administration interfaces allow users to forward and screen calls in advance or in real time. The phone services enable users to check e-mail, voice mail, calendar, and personal contact information using the large, pixel-based LCD and interactive soft keys on the Cisco IP Phone 7940 or 7960.

Key Features

- Ubiquitous Access: Cisco Personal Assistant with Speech Recognition and IP Phone Productivity Services integrate with Cisco CallManager, Cisco Unity, and Microsoft Exchange within Cisco AVVID to streamline communications
- Automatic Speech Recognition (ASR): Speech recognition interface allows users to utilize simple voice commands to perform tasks such as retrieval, replying, recording, and deletion of voice messages; Entries can be dialed from personal address books or the corporate enterprise Lightweight Directory Access Protocol (LDAP) directory; Users can synchronize their Microsoft Exchange contact lists with their personal address books for quick name-dialing and ad-hoc group conferencing; Access to sensitive features such as voice mail is controlled by user authentication
- Manage Inbound and Outbound Calls (Rules-Based Routing): Using a Web interface to create rules, users can forward and screen calls based on caller identification, time of day, and meeting schedules; With "follow me," a special rule that uses speech recognition, users can forward all calls to a phone number immediately; Users can activate sets of pre-created rules from any telephone
- CalendarView: Users can keep track of appointments right on the IP phone, directly from the Microsoft Exchange server with no synchronization necessary. In addition, users can choose to be notified of an upcoming event on the phone display or by pager
- MailView: Cisco Personal Assistant presents users with access to e-mail and Cisco Unity voice-mail messages in the inboxes on the corporate messaging server. Users can access messages from a conference room, lobby phone, or colleague's phone, as well as their own. Any operation performed on the messages using MailView is automatically reflected in Microsoft Exchange and Cisco Unity; Cisco Personal Assistant interfaces with Microsoft Exchange and IMAP 4 message stores for MailView features.

Specifications

Feature	Cisco Personal Assistant
Platform	Cisco Media Convergence Server MCS-7825H-2.2-EVV1 and MCS-7835H-2.4-EVV1
Web Server Requirements for IP Phone Productivity Services Platform	Basic Web Server: Microsoft IIS 4.0 or later Separate server for Cisco Personal Assistant Server and Speech Recognition Server
Software Compatibility	Cisco CallManager 3.1+. 3.2+, and 3.3+ Cisco Unity 2.46+,3.0+, and 4.0+ for voice-mail features Microsoft Exchange 5.5 and Exchange 2000 for calendar, e-mail, contact synchronization features

Selected Part Numbers and Ordering Information[1]

Cisco Personal Assistant

SW-PASR1.3-SVR2S	Cisco Personal Assistant 1.2 Server Software with Speech Recognition[2]
SW-PERSPROD-USR=	Personal Productivity User License
SW-PERSPROD-USR10=	Personal Productivity 10 User License
SW-PASR1-KX=	Cisco Personal Assistant 1.2, Expansion Speech Recognition Session[3]

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

[2] Cisco Personal Assistant can be purchased with an MCS-7825H-2.2-EVV1 or an MCS-7835H-2.4-EVV1 media convergence server.

[3] Various session combinations available.

For More Information

See the Cisco Personal Assistant Web site: **http://www.cisco.com/go/personalassist**

Additional Cisco IP Telephony Applications

Cisco SRS Telephony

Survivable Remote Site Telephony (SRS Telephony) provides key backup telephony functions at remote branch office routers if connectivity to the centrally-located Cisco CallManager fails (i.e. WAN link is interrupted). In this case the SRS Telephony-enabled router will take over and provide basic telephony service (including off-net calls to 911). Introduced in Cisco IOS Release 12.1.5YD, the application is ideal for enterprise organizations looking to cost-effectively deploy IP telephony in their branch office location. Cisco IOS Release 12.2(13)T added SRS Telephony 2.0 features on Cisco 1751, 1760, 2600, 2600 XM, 2691, 3600, 3725/3745, IAD 2400, Catalyst 4000 AGM, and Cisco 7200 series of routers. SRS Telephony 2.1 features are available in 12.2(11)YT on Cisco 1751, 1760, 2650, 2600XM, 2691, 3640/3640A, 3660, and Cisco 3725/3745 routers.

SRS Telephony 2.0 features: Huntstop support; Music/Tone on Hold; Class of Restriction; Distinctive Ringing; Global forwarding to voicemail across PSTN during Cisco CallManager fallback; TCL based simple AA and IVR on local gateway (SRS Telephony router); Transfer across H323 network of Cisco endpoints; Alias lists for single number to be designated for unregistered phones

SRS Telephony 2.1 features: International language support; Call forward no-answer/busy to Unity server with Personal Greeting; Cisco 7914 and 7935 support; VG248 support

For More Information

See the Cisco SRS Telephony Web site: **http://www.cisco.com/go/srs**

Cisco IP Phone Messenger

The Cisco IP Phone Messenger (IPPM) is a productivity application, providing enhanced, real-time collaboration for Cisco AVVID IP Communications systems. Cisco IPPM extends the benefits of Instant Messaging and Presence to Cisco CallManager networks, allowing users to send and receive instant messages on Cisco 7940 and 7960 IP phones. Cisco IPPM interworks with IBM Lotus Sametime and MSN Messenger clients and supports the IETF SIMPLE (RFC-3428) protocol for instant messaging and presence. IPPM 1.1 requires Cisco CallManager release 3.2 or later and is supported on the Cisco 7825 and 7835 Series Media Convergence Servers.

For More Information

See the Cisco IP Communications Web site:
http://www.cisco.com/go/ipcommunications

Cisco IP SoftPhone

Cisco IP SoftPhone 1.3 is a PC based application that allows you to use your phone extension from wherever you connect to your corporate IP network, even over the Internet when using a VPN client.

It's dual mode operation allows you to either control a physical IP phone, or perform all the functions of a phone in standalone mode using your PC's soundcard or a USB audio handset or headset.

Selected Part Numbers and Ordering Information[1]

Cisco Survivable Remote Site Telephony (SRS Telephony) Licenses	
FL-SRST-SMALL	SRS Telephony Site License for the Cisco IAD 2400/2600/3620/Catalyst 4224 (up to 24 phones)
FL-SRST-MEDIUM	SRS Telephony Site License for the Cisco 3640 (up to 48 phones) or order multiple licenses for the Cisco 3660 (up to 144 phones, each supports up to 48 phones)
Cisco IP SoftPhone	
SW-IPSOFTPHONE25=	Cisco IP Softphone CD; 25 licenses (licenses also available for 1, 50, and 100 users)

For More Information

See the Cisco IP SoftPhone Web site: **http://www.cisco.com/go/softphone**

Cisco IP Manager Assistant[1]

Cisco IP Manager Assistant is a tool that allows an assistant to provide call coverage for up to five managers simultaneously. When a user is configured as an IPMA manager, they are associated with a primary and secondary assistant. The configured manager is always logged onto the service and selects the preferred assistant from the 7960 services menu. Features available to the manager are initiated from softkeys on the manage's phone. Assistant user features are initiated and managed from a PC-based application named the Assistant Console.

[1] IP Manager Assistant is available as part of Cisco CallManager 3.3 for no additional charge.

Key Features

- Manager tools: 7960 IP phone—selection of assistant from pre-configured list; Divert All, Immediate Divert, Transfer to Voice Mail, Intercept, DND, SetWatch, Assistant Watch, Call Filtering feature invocation; display of toggled feature status for Divert All, Filtering, DND, Assistant Watch and Assistant availability; speed dial and line appearance configuration for intercom functionality; Manager Desktop—secure, browser-based access to configuration for default assistant assignment, Divert All target, Immediate Divert target and filter list (CLID) configuration.
- Admin Assistant Tools: 7960 IP Phone/7914 line extender—speed dial and line appearance configuration for intercom functionality; 7960 IP phone—invocation of new softkey features including Transfer to Voice Mail and Immediate Divert, speed dial to manager's intercom line; Assistant Console application—Windows application installed on assistant PC. GUI consistent with CallManager Attendant Console application. User-sizable application window and panes

Specifications

Feature	Cisco IP Manager Assistant
Platform	Media Convergence Server (MCS)
Software Compatibility	Cisco CallManager version 3.3 Assistant Console Application—Microsoft Windows 98, NT desktop, ME, 2000 Desktop and XP

For More Information

See the Cisco Media Convergence Server Web site: **http://www.cisco.com/go/ipma**

Cisco Conference Connection

Cisco Conference Connection (CCC) is designed for small to medium enterprises and remote offices of larger enterprises. Cisco Conference Connection facilitates relevant participation regardless of location, enables faster decisions, and eliminates travel cost and time and disruptions caused by requirements for a physical conference room presence. Typical applications include service calls, project management, sales reviews, corporate announcements, customer and employee training, and other business meetings. This application is ideal for enterprieses trying to increase productivity while reducing expense. Simple web-based interface enables employees to manage their conference schedules and eliminates the service charges to conference service providers.

For More Information

See the Cisco Conference Connection Web site:
http://www.cisco.com/en/US/products/sw/voicesw/ps752/index.html

Cisco MCS 7800 Series Media Convergence Servers

Cisco MCS 7815I-2000

The Cisco MCS 7815I-2000 provides an entry level tower server equipped with an Intel Pentium™ 4 2000MHz processor, 40GB ATA hard drive and single non-hot swap power supply. An optional tape backup is available on some models of the MCS 7815I-2000.

Cisco MCS 7825H-2266

The Cisco MCS 7825H-2266 provides an entry level rack mount server that occupies only one rack mounting space. This server is equipped with an Intel Pentium™ 4 2266MHz processor, 40GB ATA hard drive and a single non-hot swap power supply. An optional tape backup is available on some models of the MCS 7825H-2266.

Cisco MCS 7835H-2400 and Cisco MCS 7835I-2400

These Cisco MCS platforms provide a highly available mid-level rack mounted server solution that is equipped with an Intel Prestonia Xeon™ 2400MHz processor, up to six hot-swap Small Computer Systems Interface (SCSI) hard disks, a Redundant Array of Independent Disks (RAID) 1/0 Controller, hot swap fans and redundant hot swap power supplies. An optional tape backup is available for some models of the MCS 7835H-2400 and MCS 7835I-2400.

Cisco MCS 7845H-2400 and Cisco MCS 7845I-2400

These Cisco MCS platforms provide a powerful and highly reliable high level rack mounted server solution that is equipped with two Intel Prestonia Xeon™ 2400MHz processors, up to six hot-swap SCSI hard disks, RAID 1/0 controller, redundant hot swap fans and redundant hot swap power supplies. An optional tape backup is available for some models of the MCS 7845H-2400 and MCS 7845I-2400.

Specifications

Cisco MCS-7815I-2000	Cisco MCS-7825H-1266	Cisco MCS-7835H-2400	Cisco MCS-7835I-2400	Cisco MCS 7845H-2400	Cisco MCS 7845I-2400
Intel Pentium® 4 2000-MHz processor 512KB L2 Cache 512MB SDRAM 40GB ATA/100 Hard Disk 1.44MB Floppy Disk DVD Drive Integrated ATA Controller Single 10/100/1000 Ethernet NIC Tower System with optional rack mount kit.	Intel Pentium® 2266-MHz processor 512KB L2 CacheSDRAM is configuration dependant Hard Disk is configuration dependant 1.44MB Floppy Disk DVD Drive Hard Disk Controller is configuration dependant Dual 10/100/1000 Ethernet NIC1U Rack Mount System	Intel Xeon® 2400-MHz processor 512KB Cache SDRAM is configuration dependant Hard Disk is configuration dependant SCSI Controller. Dual 10/100/1000 Ethernet NIC2U Rack Mount System.	Intel Xeon® 2400-MHz processor 512KB Cache SDRAM is configuration dependant Hard Disk is configuration dependant SCSI Controller. Dual 10/100/1000 Ethernet NIC2U Rack Mount System	Dual Intel Xeon® 2400-MHz processor 512KB Cache SDRAM is configuration dependant Hard Disk is configuration dependant SCSI Controller. Dual 10/100/1000 Ethernet NIC2U Rack Mount System	Dual Intel Xeon® 2400-MHz processor 512KB Cache SDRAM is configuration dependant Hard Disk is configuration dependant SCSI Controller. Dual 10/100/1000 Ethernet NIC2U Rack Mount System

Selected Part Numbers and Ordering Information[1]

7679 3

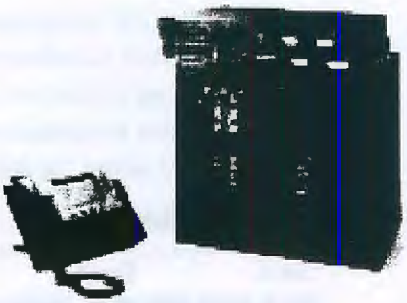
Cisco Media Convergence Server 7815I-20001[1]	
MCS-7815I-2.0-EVV1; CS-7815I-2.0-ECS1	Cisco Media Convergence Server 7815I-2000
Cisco Media Convergence Server 7825H-2266	
MCS-7825H-2.2-EVV1; MCS-7825H-2.2-ECS1	Cisco Media Convergence Server 7825H-2266
Cisco Media Convergence Server 7835H-2400	
MCS-7835H-2.4-EVV1; MCS-7835H-2.4-ECS1	Cisco Media Convergence Server 7835H-2400
Cisco Media Convergence Server 7835I-2400	
MCS-7835I-2.4-EVV1; MCS-7835I-2.4-ECS1	Cisco Media Convergence Server 7835I-2400
Cisco Media Convergence Server 7845H-2400	
MCS-7845H-2.4-EVV1; MCS-7845H-2.4-ECS1; MCS-7845H-2.4-ECS2	Cisco Media Convergence Server 7845H-2400
Cisco Media Convergence Server 7845I-2400	
MCS-7845I-2.4-ECS1; MCS-7845I-2.4-ECS2	Cisco Media Convergence Server 7845I-2400
Cisco Media Convergence Server 7855I-1500	
MCS-7855I-1.5-ECS1; MCS-7855I-1.5-ECS2	Cisco Media Convergence Server 7855I-1500
Cisco Media Convergence Server 7865I-1500	
MCS-7865I-1.5-ECS1; MCS-7855I-1.5-ECS2	Cisco Media Convergence Server 7865I-1500

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Media Convergence Server Web site: **http://www.cisco.com/go/mcs**

Cisco ICS 7750 Integrated Communications System



The Cisco Integrated Communications System (ICS) 7750 is a versatile IP telephony and services solution that brings the benefits of converged IP services to midmarket businesses and enterprise branch offices. Call processing, voice applications, voice gateways and multiservice IP routing are integrated within the system chassis to deliver true convergence while enhancing system manageability. The modular system architecture enables expansion of call processing redundancy, voice gateway capacity, routing capacity, and IP services to deliver system availability and scalability. The ICS 7750 offers quick and cost-effective deployment of powerful applications including unified messaging, integrated Web call centers, and data/voice collaboration.

The Cisco ICS 7750 includes Cisco CallManager software, and combines an IOS-based multiservice router/voice gateway, application servers running core voice applications, Web-based management, and seamless connectivity to Cisco Catalyst switches.

Cisco Systems also offers four Cisco ICS 7750 voice packages for convenient and cost-effective entry points for customers to deploy IP telephony solutions in their LAN networks. These ICS voice packages are pre-configured to simplify ordering of the necessary voice components including voice mail for a mid-market business or branch site.

When to Sell

Sell This Product	When a Customer Needs These Features
ICS 7750 Integrated Communications System	• A branch office/midmarket business with standalone IP telephony needs from 35-500 users • An end-user customer or partner who wants a single "box" (or platform) IP telephony solution to ease deployment and/or to standardize on voice configurations across multiple sites • An existing multiservice data network customer who wants to add IP telephony functionality to create a converged network solution

Key Features

- Integrated Functionality (includes CallManager for call-processing, multiservice router/voice gateway, Web-based management, and core voice applications)
- Modular chassis architecture features 6 universal slots with hot swapability
- Modular industry-proven Cisco IOS-based Multiservice Route Processor (MRP) delivers data routing and voice trunking; ensures end-to-end QoS
- Industry-leading selection of WAN Interfaces
- World wide selection of voice interfaces
- Optional redundant power supply and uninterruptible power supply
- Optional integrated voice applications including Unity voice/unified messaging, IVR, contact center
- Integrated Web/GUI-based system management tool for simple monitoring and troubleshooting; Console and Telnet access to CLI system management
- Automated inventory, discovery, and configuration of desktop devices and applications
- Automated fault management, auto-notification of problems via e-mail or pager
- Compatible with SNMP-based management tools including CiscoWorks 2000
- N+1 CallManager clustering enables a backup Cisco CallManager to improve system availability

Specifications

Feature	Cisco ICS 7750
System Switch Processor	Fixed slot card; 10/100BaseT autosensing data switch; Two-port RJ-45 connectors; Included with each ICS 7750 system
System Alarm Processor	Fixed slot card; Two serial ports; One console port; Resource Cards; Included with each ICS 7750 system
System Processing Engine	Universal slot card; Intel Pentium III 700 MHz CPU;1 GB SRAM; 40 GB hard disk drive
Multiservice Route Processor	Universal slot card; Standard memory: 64 MB DRAM (max.128 MB); Memory upgrade (option): 16, 32, 64 MB DRAM; Standard flash memory: 16 MB Flash SIMM (max. 80 MB); Flash upgrade (options): 16, 32, 64 MB Flash; modular voice/WAN interface (VWIC) card slots per card; Advanced data networking feature support, including: VPN, IPSec 56 and 3DES, Firewall
Dimensions and Weight (HxWxD)	15.75 x 17.25 x 12.5 in. (40.005 x 43.815 x 31.75 cm)Basic configuration-1 MRP, 1 SPE, 1 SSP, 1 SAP (a total of 4 cards = 2 fixed cards + 2 universal cards) and 1 power supply): 42 lb (18.9 kg)
Mounting Options	19 in rack-mount; Standalone

Selected Part Numbers and Ordering Information[1]

Cisco ICS 7750 Voice Packages

ICS-7750-M1V	Cisco ICS 7750 FXO-M1 Analog Voice Package provides eight Foreign Exchange Office (FXO) analog voice interfaces, four analog FXS/DID ports, 25 Cisco Unity Voice Messaging mailboxes and support for up to 50 Cisco CallManager devices.
ICS-7750-TV	Cisco ICS 7750 T1 Digital Voice Package provides 24 digital voice channels (DS0s), 8 analog FXS interfaces, 50 Cisco Unity Voice Messaging mailboxes and support for up to 500 Cisco CallManager devices.
ICS-7750-BV	Cisco ICS 7750 ISDN BRI Voice Package provides four ISDN BRI interfaces (eight B channels), 50 Cisco Unity Voice Messaging mailboxes and support for up to 500 Cisco CallManager devices.
ICS-7750-EV	Cisco ICS 7750 E1 Digital Voice Package provides 30 digital voice channels (DS0s), 50 Cisco Unity Voice Messaging mailboxes and support for up to 500 Cisco CallManager devices.

Cisco ICS 77501

ICS-7750	Six-slot ICS chassis, SPE310, SSP, SAP, Power Supply & DOC-CD
SPE310=	System Processing Engine 310 (512MB RAM and Windows 2000)
MRP300=	Multiservice Route Processor 300 with two VIC/WIC slots
MRP3-8FXOM1=	Multiservice Route Processor with 8-ports FXO-M1 and one VIC/WIC slot
MRP3-8FXS=	Multiservice Route Processor with 8-ports FXS and one VIC/WIC slot
MRP3-16FXS=	Multiservice Route Processor with 16-ports FXO-M1
UPS-BASE-UNIT=	UPS with Standard Battery Pack, Ethernet Card (120 V for North America)
UPS-BATT-PACK=	Additional External Battery Pack for UPS Base Unit
PWR-AC-7750=	AC Power Supply for ICS 7750 Chassis
FAN-TRAY-7750=	Fan Tray for ICS-7750
ICS-7750-CHASSIS=	ICS-7750 Six-slot chassis & Fan Tray
SAP-7750=	System Alarm Processor for ICS 7750
SSP-7750=	System Switch Processor for ICS 7750

Cisco ICS 7750 WAN Interface Card (WIC) Modules (for MRP cards)

WIC-1DSU-T1=	1-Port T1/Fractional T1 DSU/CSU WAN Interface Card
WIC-1T=	1-Port Serial (T1/E1) Async/Sync WAN Interface Card
WIC-2T=	2-Port Serial (T1/E1) Async/Sync WAN Interface Card
WIC-2A/S=	2-Port low-speed Serial (up to 128kbps) Async/Sync WAN Interface Card spare
WIC-1DSU-56K4=	1-Port 4-Wire 56Kbps DSU/CSU WAN Interface Card
WIC-1B-S/T=	1-Port ISDN BRI S/T WAN Interface Card (dial and leased line)
WIC-1B-U=	1-Port ISDN BRI U with NT-1 WAN Interface Card dial and leased-line

Cisco ICS7750 Voice Interface Card (VIC) Modules (for MRP cards)

VIC-2FXS	Two-port FXS voice/fax interface card
VIC-4FXS/DID	Four-port FXS or DID voice/fax interface card (ports can be configured for either FXS or DID)
VIC-2DID	Two-port DID voice/fax interface card
VIC-2FXO	Two-port FXO voice/fax interface card
VIC-2FXO-M1	Two-port FXO voice/fax interface card with battery reversal and caller ID (for North America)
VIC-2FXO-M2	Two-port FXO voice/fax interface card with battery reversal and caller ID (for Europe)
VIC-2FXO-M3	Two-port FXO voice/fax interface card with battery reversal and caller ID (for Australia)
VIC-4FXO-M1	Four-port FXO voice/fax interface card with battery reversal and caller ID (for N. America)
VIC-2E/M	Two-port E&M voice/fax interface card
VIC-2BRI-NT/TE	Two-port IDSN BRI (NT & TE) voice interface card
VWIC-1MFT-T1	One-port T1/fractional T1 multiflex trunk with CSU/DSU (for CAS or PRI)
VWIC-2MFT-T1	Dual-port T1/fractional T1 multiflex trunk with CSU/DSU (for CAS or PRI)
VWIC-1MFT-E1	One-port E1/fractional E1 multiflex trunk with CSU/DSU (for PRI)
VWIC-2MFT-E1	Dual-port E1/fractional E1 multiflex trunk with CSU/DSU (for PRI)

Cisco ICS 7750 Packet Voice/Fax DSP Modules (for MRP cards)

PVDM-256K-4=	4-Channel Packet Voice/Fax DSP Module
PVDM-256K-8=	8-Channel Packet Voice/Fax DSP Module
PVDM-256K-12=	12-Channel Packet Voice/Fax DSP Module
PVDM-256K-16=	16-Channel Packet Voice/Fax DSP Module
PVDM-256K-20=	20-Channel Packet Voice/Fax DSP Module

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the ICS 7750 Web site: **http://www.cisco.com/go/ics7750**

Cisco IAD 2400 Series Integrated Access Device with IOS Telephony Service (ITS)[1]

The Cisco IAD 2400 Series integrated access devices (IADs) combine data, voice, and video services over IP and ATM networks to provide cost-effective and efficient means of delivering high-speed Internet and voice services to small- and medium-sized business customers--all in a small (1 RU) system. When configured with optional ITS software, the IAD 2400 is ideal for delivering converged LAN IP telephony in small office environments (5-20 phones) that do not require CallManager functionality.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco IAD 2400 Series	Business-class, fully integrated access device • IOS Telephony Service (ITS), ideal for small offices (5-20 phones) that do not need Cisco CallManager capabilities • Support for standard phones and IP phones on a single platform • 8 FXS/16 FXS/16FXS+8FXO analog voice ports and 1 T1 digital voice port models • T1-PPP, FR, HDLC, ATM, ADSL and G.shdsl WAN interfaces

Key Features

- Combines high-speed Internet access and toll-quality voice services on single IOS-based platform (ITS introduced in Cisco IOS Release 12.1(5)YD)
- Offers TDM, VoIP, and VoATM (AAL2) on a single platform
- Seamless migration of customers from TDM-based GR-303 to packet-based GR-303 networks or to call agent-based networks
- Automated remote installation and configuration enabled via Simple Network-enabled Auto Provisioning (SNAP) and the Cisco Configuration Express tool

Competitive Products

- Adtran: TA850, TA750, TA600
- Carrier Access: Adit 600
- Coppercom: MXR 400
- RAD: LA-110, LA-140
- Verilink (formerly Polycom): NetEngine 6200, 7200
- Wave7 Optics: LMG-B

Specifications

Feature	IAD 2421	IAD 2423	IAD 2424
Fixed LAN Ports	1-port Ethernet (10BASE-T)	Same as IAD 2421	Same as IAD 2421
Fixed WAN Ports	1-port T1	1-port ADSL	1-port G.SHDSL
Voice Ports	Analog: 8FXS, 16FXS, 16FXS+8FXO; Digital: 1 T1	Analog: 8FXS	Analog: 8FXS, 16FXS, 16FXS+8FXO; Digital: 1 T1
Processor Speed (type)	80 MHz (RISC)	Same as IAD 2421	Same as IAD 2421
Flash Memory	16 MB (Default); 32 MB (Max)	16 MB (Default); 32 MB (Max)	16 MB (Default); 32 MB (Max)
DRAM Memory	64 MB	64 MB	64 MB
Dimensions (HxWxD)	1.7 x 17.5 x 11.3 in.	Same as IAD 2421	Same as IAD 2421

For More Information

See the Cisco IAD 2400 Web site: **http://www.cisco.com/go/2400**

[1] IP Keyswitch capabilities also available with 2600 and 3600 series routers; see IP Keyswitch Web site: http://www.cisco.com/go/keyswitch

Cisco Voice Gateways

Voice Gateways interface directly to PBXs or public telephone networks to carry voice traffic across IP networks—by converting IP calls to standard telephony calls and vice versa. They provide connectivity between packet telephony and legacy telephony such as PSTN, PBX, fax machines, and other devices.

Cisco's full line of multiservice routers can also add analog and digital voice gateway functionality through the use of network modules and voice interface cards[1], such as the Catalyst 6000 Family FXS Analog Interface Module.

Cisco offers the Cisco VG248 dedicated voice gateway.

Cisco VG248 Voice Gateway

The Cisco VG248 Voice Gateway is a 1 unit high rack mountable device allowing 48 analog devices (phones, fax machines & modems) to be used with Cisco Call Manager. It enables organizations with large numbers of analog phones (hotels, universities, hospitals, etc.) to deploy IP Telephony while maintaining the investment in legacy handsets. The analog lines are full featured (caller id, message waiting lights, feature codes) and the price per port is competitive with a legacy PBX.

The VG248 will generate SMDI for the attached analog ports allowing connection to a Cisco Call Manager network through legacy voicemail systems. It shares existing SMDI based voicemail systems between the Cisco Call Manager and the legacy PBX.

Selected Part Numbers and Ordering Information

Cisco VG 248 Voice Gateway

VG248	48 Port Voice over IP analog phone gateway

For More Information

See the Cisco Voice Gateways Web site: **http://www.cisco.com/go/voicegate**

Cisco IP/VC 3500 Series Videoconferencing Products

The IP/VC 3500 series is for enterprises and service providers who want a reliable, easy-to-manage, cost-effective network infrastructure for videoconferencing over their IP networks. They consist of the IP/VC 3511 Multipoint Control Unit (MCU, also known as a "video bridge"), the IP/VC 3521 and 3526 H.320 to H.323 Gateways and the IP/VC 3540-Series Videoconferencing System. The Cisco IP/VC product family works with H.323-standards-based videoconference client devices from a variety of vendors and integrates with legacy H.320 networks.

- The Cisco IP/VC 3511 Multipoint Control Unit (MCU) is a 1RU stack/rack-mount system enabling adhoc videoconferences between three or more endpoints. Multiple participants in multiple locations attend the same meeting with real-time interactivity. It is suitable for small to medium enterprises and remote branch offices in larger enterprises
- The IP/VC 3521 and the IP/VC 3526 Videoconferencing Gateways are also 1RU stack/rack-mount systems that translate between H.320 and H.323 protocols. The IP/VC 3521 provides up to four BRI interfaces and the IP/VC 3526 provides one ISDN T1/E1 PRI interface

[1] Please see the 1700, 2600, 3600, 7200, 5x00 series in Chapter 1—Routers, Chapter 7—Access Products.

- The IP/VC 3540 Videoconferencing System integrates multipoint control units, and gateways I onto a single platform for cost-effective deployment of IP-centric videoconferencing networks. In addition, the IP/VC 3540 platform offers T.120 data conferencing through an optional collaboration server. Customers can add the Rate Matching module which enhances the video composition of any multipoint conference. Enhanced features such as Rate Matching, a number of robust Continuous Presence formats and audio transcoding are available
- The Multimedia Conference Manager (MCM) software is part of Cisco IOS Software and available across a wide range of Cisco router platforms, including the Cisco 2600/2600XM, 3600, 3700, and 7200 series. As a gatekeeper/proxy, it enables network managers to control and secure bandwidth and priority settings for H.323 videoconferencing services

Selected Part Numbers and Ordering Information[1]

Cisco IP/VC 3500 Series Videoconferencing Products

IPVC-3511-MCU	IP/VC 3511 H.323 Videoconference Multipoint Control Unit
IPVC-3521-GW-4B	IP/VC 3521 H.320-H323 Videoconferencing Gateway with 4 BRI ports
IPVC-3526-GW-1P	IP/VC 3526 H.320-H.323 Videoconferencing. Gateway-1 PRI
IPVC-3540-MC03A	IP/VC 3540 MCU Module - 30 Sessions - (also available in 60 and 100 session capacities)
IPVC-3540-XAM03	IP/VC 3540 Audio Transcoder for 30 session MCU (also available for 60 session MCU)
IPVC-3540-RM	IP/VC 3540 Rate Matching Module (allows different rates in the same conference)
IPVC-3540-GW2P	IP/VC 3540 H.320 to H.323 Gateway Module
IPVC-3540-XAG	IP/VC 3540 Gateway Audio Transcoder
IPVC-3540-AS	IP/VC 3540 Application Server (CPU required for T.120 Data Conferencing Server
IPVC-3540-DS03	IP/VC 3540 T.120 Data Conferencing Server software (also available in 60 sessions)
MCM Images	IP/H323 (Routers: 2600, 3600, 3700)
IOS 12.2(11)T	Enterprise Plus/ H323 MCM (Routers: 2600, 3600, 3700) Enterprise MCM (Routers: 7200)

[1] This is only a small subset of all parts available. Some parts have restricted access or are not available through distribution channels.

For More Information

See the IP/VC 3500 series Web site: **http://www.cisco.com/go/ipvc**

Cisco IP/TV 3.4

Cisco IP/TV® 3.4 delivers a complete, highly scalable, bandwidth-efficient solution for high-quality video communications over enterprise networks. Cisco IP/TV supports live video, scheduled video, video on demand (VOD), synchronized presentations and screen captures, and a wide range of video management functions. The solution enables a broad spectrum of applications for enterprise communications including training, corporate communications, business TV, and distance learning.

Cisco IP/TV 3.4 are purchased as Cisco IP/TV 3400 Series Server appliances or software for third party servers. The Cisco IP/TV 3400 Series servers contain pre-configured software, preinstalled capture cards, network interface cards, and device drivers. The Cisco IP/TV 3400 Series includes the IP/TV 3412 Control Server, the IP/TV 3425 and 3425A Broadcast Servers, the IP/TV 3432 Archive Server, and the IP/TV 3417 Video Starter System. This product family offers a range of choices to best suit large-scale enterprise applications, performance requirements, and bandwidth availability.

Selected Part Numbers and Ordering Information[1]

Cisco IP/TV 3400 Series Video Servers	
IPTV-3412-CTRL	Cisco IP/TV 3412 Control Server
IPTV-3425-BCAST-M	Cisco IP/TV 3425 MPEG-1, MPEG-2 Full D1 Broadcast Server
IPTV-3425A-BCAST-M	Cisco IP/TV 3425 MPEG-1 Broadcast Server
IPTV-3432-ARCH	Cisco IP/TV 3432 Archive Server
IPTV-3417-START-M	Starter Kit
Cisco IP/TV Software	
IPTV-CM-3.4	IP/TV Content Manager
IPTV-SERV-3.4	Broadcast/Archive Server
IPTV-SERV-MP4-3.4	Server w/ MPEG-4 card & license
IPTV-START-HD1-3.4	Starter Kit

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the IP/TV 3400 series Web site: **http://www.cisco.com/go/iptv**

Web Collaboration—Cisco Web Collaboration Option

The Cisco Web Collaboration Option enables businesses to combine the personal value of human interaction with the information value of the Web-creating a powerful environment for driving increased sales, exceptional service, and customer satisfaction.

The Cisco Web Collaboration Option allows you to add "click-for-help" buttons on your Web site that enable customers to interact with your contact center agents over the Web while conducting a voice conversation (PSTN or Voice over IP [VoIP]) or text chat. Contact center agents and callers can share Web pages-including personalized or dynamically generated pages, complete forms in a collaborative fashion, and share any Windows desktop application using nothing more than a Web browser. By facilitating effective, personalized assistance designed to greatly enhance the customer experience, the Cisco Web Collaboration Option is an ideal solution for both sales- and service-oriented contact centers.

The Cisco Web Collaboration Option can be deployed in a pure IP environment or can be seamlessly integrated with your organization's existing telephony infrastructure to provide automated, blended delivery of phone and Web-based inquiries.

Selected Part Numbers and Ordering Information[1]

Cisco IP/TV 3400 Series Video Servers	
CCS-CCSSVR	Cisco Web Collaboration and Media Blender Software

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco Collaboration Server Web site: **http://www.cisco.com/go/ccs**

E-Mail Response Management–Cisco E-mail Manager

Cisco E-Mail Manager is a comprehensive, enterprise-class solution for managing high volumes of customer inquiries submitted to your company mailboxes or Web site. Based on customizable business rules, Cisco E-Mail Manager accelerates the response process by automatically directing messages to the right agent or support team, categorizing and prioritizing messages, suggesting relevant response templates, and, if desired, sending automated replies. A full-featured, browser-based interface provides your agents with the productivity tools and knowledge resources they need to provide fast, accurate and personalized responses to your customers. Cisco E-Mail Manager gives managers the queue management, reporting and outbound marketing tools they need to ensure that desired service standards are met, gain valuable insight into customer needs and generate new revenue opportunities.

Whether you are building a customer support system from the ground up or integrating with existing organizational structures and legacy systems, Cisco E-Mail Manager's uniquely flexible, extensible and scalable design delivers a cost-effective, easy-to-implement strategy for building customer relationships over the Internet.

Selected Part Numbers and Ordering Information[1]

Cisco Email Manager	
CEM-SVR-W	Cisco Email Manager Server (Win 2K)
CEM-AGT	Cisco Email Manager Agent License

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

Cisco Emergency Responder

Cisco Emergency Responder revolutionizes enterprise telephony support for E9-1-1 in North America, E1-1-2 in Europe, and other emergency telephone services across the globe. Traditional PBX E9-1-1 implementations in North America support "automatic location identification" of emergency callers through daily manual database update processes, which limit the frequency of location updates and increase the likelihood of update errors. The Cisco Emergency Responder software application works with Cisco CallManager to automatically track the location of Cisco IP phones in enterprise campuses, route emergency calls to an appropriate public safety answering point (PSAP), and provide the location of the caller to the Public Safety Answering Point (PSAP).

Cisco ER performs these functions without requiring tedious manual database updates after phone moves/adds/changes, which significantly reduces the time, headcount, and costs associated with traditional PBX E9-1-1 maintenance. While some vendors may automate location updates, they still require manual PBX configuration changes to trigger the updates. The Cisco ER solution, when coupled with the automated phone moves/adds/changes features in Cisco CallManager, is the first in the industry to completely automates the phone move process while maintaining E9-1-1 and location data integrity.

In addition, Cisco ER can use email/pager messaging, telephone calls, and auto-refreshing webpage updates to notify on-site security operations personnel and third-party agencies of emergency calls in progress.

Key Features

- Meets and exceeds traditional E9-1-1 requirements
- Automates all user and phone moves, adds, and changes; Enables users and phones to move an unlimited number of times per day
- Avoids the expense and burden of daily PS-ALI record uploads
- Avoids daily error-prone documentation and database updates
- Enables quicker and more effective emergency response from onsite personnel and public agencies
- Provides configuration auditing to facilitate responsible change management and investigative or legal processes
- Provides call history logs for capacity planning, management of emergency call abuse, and incident documentation
- Compatible with any emergency number

Specifications

Feature	Cisco Emergency Responder
Supported Platform	Cisco Media Convergence Server, MCS-7835-1266 and MCS-7825-1133
System Capacity	A single Cisco Emergency Responder server supports 10,000 phones and 30,000 Ethernet switch ports. Additional scalability parameters include 500 Emergency Response Locations (ERLs)- locations that can be uniquely identified to a Public Safety Answering Point (PSAP)- as well as 500 manually entered endpoints such as analog or proprietary phones or H.323 clients. Cisco recommends a second Emergency Responder server to form a fully redundant Cisco Emergency Responder Group with the same capacity and increased availability compared with a single Cisco Emergency Responder server. Larger campuses and distributed systems are supported via a network of Cisco Emergency Responder groups called a Cisco Emergency Responder Cluster.
Configurable Elements	
Cisco CallManager	Call routing and digit manipulation to forward user-initiated emergency calls and PSAP return calls to and from Cisco Emergency Responder as appropriate
Cisco Emergency Responder	System administration interface-for access to all configuration components or oversight of outsourced vendors LAN administration interface-for IT LAN group or an outsourced vendor Emergency Response Location (ERL) administration interface-for IT telecom group or an outsourced vendor
Other Components	Configure e-mail account on a Simple Mail Transfer Protocol (SMTP) Internet mail server for use by Cisco Emergency Responder Configure an email-to-pager gateway, or use an email paging service Configure a PS-ALI transfer application provided by the PS-ALI database service provider (often requires a dialup modem connection) Provision an E9-1-1 capable voice trunk (Centralized Automated Message Accounting [CAMA] or Primary Rate Interface [PRI]) through a local exchange carrier
Supported Switches[1]	Cisco Catalyst 2950, 3500, 3550, 4000, 4500, 6500 Series

[1] Check for updates on CCO, and following is list of tested switch platforms at time of printing

Selected Part Numbers and Ordering Information[1]

Cisco Emergency Responder

SW-ER1.1-SVR	Cisco Emergency Responder software (MCS platforms), including 100 user licenses
SW-ER1.1-SVR-CPQ=	Cisco Emergency Responder software (Compaq platforms), including 100 user licenses
SW-KEY-ER1.1-USER=	Incremental single-user license key for Cisco Emergency Responder

[1] Redundant user licenses are not required when ordering redundant CER servers for a single CER group.

For More Information

See the Cisco Emergency Responder Web site: **http://www.cisco.com/go/cer**

Cisco ATA Series of Analog Telephone Adaptors

The Cisco ATA 186 and 188 Analog Telephone Adaptors bring analog telephones into the networked world. The Cisco ATA series of products address the low-end product portfolio need by targeting the enterprise, business local services, small-office environment and the emerging managed voice services market. These cost effective handset-to-Ethernet adaptors enable analog devices, such as phones and fax machines, to support voice-over-IP (VoIP) services. The Cisco ATA 186 is equipped with, and a single RJ-45 Ethernet port. The Cisco ATA 188 has two RJ-11 voice ports and two RJ-45 ports. The internal Ethernet switch allows for a direct connection to a 10/100BASE-T Ethernet network and connectivity to a co-located PC or other Ethernet-based device via the RJ-45 ports.

Both models ship with a bootload image and must be upgraded to a signaling firmware image available on Cisco.com before deployment. Cisco ATAs can be configured[1] to use the standards-based Voice over IP (VoIP) protocols H.323, Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP) and Skinny Client Control Protocol (SCCP).

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco ATA Series of Analog Telephone Adaptors	• Enable analog devices, such as phones and fax machines, to support Voice over IP services by converting the analog signal into an IP signal • Continue use of existing analog phones with IP network

Key Features

- Auto-provisioning with Trivial File Transfer Protocol (TFTP) provisioning servers
- Automatic assignment of IP address, network route IP, and subnet mask via Dynamic Host Configuration Protocol (DHCP)
- Optional web configuration through built-in Web server
- Optional touch-tone telephone keypad configuration with voice prompt
- Administration password to protect configuration and access
- Advanced pre-processing to optimize full-duplex voice compression
- High performance line-echo cancellation eliminates noise and echo
- Voice activity detection (VAD) and comfort noise generation (CNG) save bandwidth by delivering voice, not silence
- Dynamic network monitoring to reduce jitter artifacts such a packet loss

[1] Two softrware image combinations are available on Cisco.com: H.323/SIP and MGCP/SCCP. MGCP/SCCP image includes the letters, ms, in its name.

Specifications

Feature	Cisco ATA 186	Cisco ATA 188
Telephone and network interfaces	2 RJ-11 FXS ports 1 RJ-45 interface for network connection	2 RJ-11 FXS ports 1 RJ-45 interface for network connection 1 RJ-45 "switch port" for connection to PC or another downstream Ethernet port
Dimensions (H x W x D)	1.5 x 6.5 x 5.75 in. (3.8 x 16.5 x14.6 cm)	1.5 x 6.5 x 5.75 in. (3.8 x 16.5 x14.6 cm)
Weights	15 oz (425 gm)	15 oz (425 gm)
Voice-over-IP (VoIP) protocols	H.323 v2; H.323 v4; SIP (RFC 2543); MGCP 1.0 (RFC 2705); MGCP 1.0/network-based call signaling (NCS) 1.0 Profile; MGCP 0.1; SCCP	H.323 v2; H.323 v4; SIP (RFC 2543); MGCP 1.0 (RFC 2705); MGCP 1.0/network-based call signaling (NCS) 1.0 Profile; MGCP 0.1; SCCP

Selected Part Numbers and Ordering Information[1]

Cisco ATA Series of Analog Telephone Adaptors	
ATA186-I1	Cisco ATA 186 2-port adaptor, 600 ohm impedance
ATA186-I2	Cisco ATA 186 2-port adaptor, complex impedance (270 ohm in series with 750 ohm and 150 nF in parallel)
ATA188-I1	Cisco ATA 188 2-port adaptor with switch, 600 ohm impedance
ATA188-I2	Cisco ATA 188 2-port adaptor with switch, complex impedance (270 ohm in series with 750 ohm and 150 nF in parallel)
Cisco ATA Series of Analog Telephone Adaptors Power Supply Cables	
ATACAB-NA	ATA power supply cable for North American-style power systems
ATACAB-EU	ATA power supply cable for Continental European-style power systems
ATACAB-UK	ATA power supply cable for United Kingdom
ATACAB-AR	ATA power supply cable for Argentina
ATACAB-JP	ATA power supply cable for Japan

[1] Some countries have telephone networks that list multiple impedance requirements. It is important to closely approximate the impedance of the typical handsets used in the region when selecting the proper configuration. The incorrect choice may lead to poor echo cancellation performance.

For More Information

See the Cisco ATA Series Web site: **http://www.cisco.com/go/ata186**

CHAPTER 5

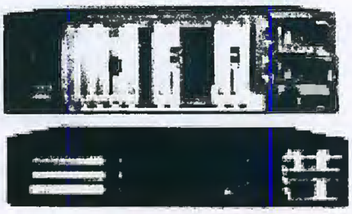
VPN and Security Products

VPN and Security Products at a Glance

Product	Features	Page
Cisco PIX Firewall	Market-leading, purpose-built appliances which provide broad range of integrated security services • Robust stateful inspection firewalling with application awareness • Highly scalable remote access and site-to-site VPN • Intrusion protection with for real-time response to network attacks • Award-winning stateful failover for enterprise-class resiliency	5-2
Cisco IOS Firewall	• Tightly integrated with IOS VPN and advanced routing technologies • Stateful packet filtering via context-based access control (CBAC) • Inline Intrusion detection for real-time response to network attacks • Dynamic, network-to network, per-user authentication and authorization via TACACS+ and RADIUS	5-5
Firewall Blade for Catalyst 6500	Firewall Module is a high performance integrated stateful firewall solution for Catalyst 6500 family of switches with performance exceeding 5GB. It is based on proven PIX technology while providing the following benefits to the customers • Investment protection • Low cost of ownership • Ease of use • Operational Consistency • Scalability See the Catalyst 6500 Series Switch in Chapter 2: LAN Switching, page 2-20 , for more information	2-20
Cisco VPN 3000 Family	Remote access Virtual Private Network platform • Has models for all size companies, from small to large enterprise organizations • Reduces communications expenditures • Enables users to easily add capacity and throughput	5-6
Cisco IDS Network Sensor	Network-based, real-time intrusion detection system capable of monitoring an entire enterprise network: • Distributed intrusion detection system capable of directing and forwarding alarms between local, regional, and headquarters-based monitoring consoles • Scalable architecture to allow the deployment of large numbers of sensors in order to provide comprehensive security coverage in large networks with performance requirements from T1 to gigabit environments • Cisco IDS Module enables customers to perform both security monitoring and switching functions within the same chassis • CTR (Cisco Threat Response) delivers patented adaptive scan techniques to minimize false alarms	5-8
Cisco Security Agent	The Cisco Security Agent provides threat protection for desktop and server computing systems by identifying and preventing malicious activity. By acting on threats or attacks before they can occur, Cisco Security Agent removes known and unknown security risks to enterprise networks and applications: • The Cisco Security Agent aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent package • Protects against know and unknown attacks on both servers and desktops	5-10
Cisco 7100 Series	Large branch and central site VPN router • Comprehensive suite of VPN services, including encryption, tunneling, firewall, and bandwidth management • Embedded I/O for ease of deployment • Service module slot for IPSec and PPTP encryption coprocessing • Dedicated Site-to-Site VPN router	5-11

Product	Features	Page
Cisco Secure Access Control Server (ACS) for Windows	Controls the authentication, authorization, and accounting (AAA) of users and administrators to network devices and services • Operates as a centralized Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) server • Supports LDAP user authentication • Data replication and backup services • Flexible user and group policy controls • Support for Cisco 802.11x Catalyst Switch and Wireless solutions • Extensible Authentication Protocol (EAP) enhancements to support Protected EAP (PEAP) for wireless LANs • All administrative access is encrypted with SSL	5-14
Cisco Secure User Registration Tool (URT)	Identifies users within the network and creates user registration policy bindings that help support mobility and tracking: • Ensures that users are associated with their authorized subnet/VLAN • Addresses the challenges associated with campus user mobility • Supports Web-based authentication for Windows, Macintosh, and Linux client platforms • Secure user access to the VLAN with MAC address-based security option • Option to allow multiple users connected to a hub to access a VLAN served by a single switch port	5-15
CiscoWorks VPN/Security Management Solution	Combines general device management tools for configuring, monitoring, and troubleshooting enterprise networks with powerful security solutions for managing virtual private networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS). This bundle includes: Management and Monitoring Centers, Cisco IDS Host Sensor and Console, Cisco Secure Policy Manager, VPN Monitor, Resource Manager Essentials, and Cisco View See Chapter 9—Cisco IOS Software and Network Management for more information on CiscoWorks VPN/Security Management Solution	9-16
Cisco 806, 1700, 2600, 3600, 7200, 7400 and SOHO 70 Series	Wide variety of modular router platforms with options for IOS-based and hardware-enabled VPN and security support. See individual product pages and Cisco IOS Firewall Feature Set (page 5-5).	1-1

Cisco PIX Firewall Series



The world-leading Cisco PIX® Firewall Series of purpose-built security appliances provides robust, enterprise-class, integrated network security services, including stateful inspection firewalling, virtual private networking (VPN), intrusion protection, and much more-in cost-effective, easy-to-deploy solutions. Ranging from compact, "plug-and-play" desktop firewalls for small and home offices to carrier-class gigabit firewalls for the most demanding enterprise and service-provider environments, Cisco PIX Firewalls provide robust security, performance, and reliability for network environments of all sizes.

When to Sell

Sell This Product	When a Customer Needs These Features
PIX 501	• Small Office / Home Office desktop integrated security appliance • Up to 10 Mbps of firewall throughput and 3 Mbps of 3DES VPN throughput[1] • Hardware VPN client (Easy VPN Remote) • VPN concentrator services (Easy VPN Server) for up to 5 remote users • Integrated four port 10/100 Mbps switch
PIX 506E	• Remote Office / Branch Office desktop integrated security appliance • Up to 20 Mbps of firewall throughput and 16 Mbps of 3DES VPN throughput[1] • Hardware VPN client (Easy VPN Remote) • VPN concentrator services (Easy VPN Server) for up to 25 remote users • Maximum of two 10BASE-T Ethernet interfaces • OSPF dynamic routing support

Sell This Product	When a Customer Needs These Features
PIX 515E	• Small-to-Medium Business (SMB) integrated security appliance • Up to 188 Mbps of firewall throughput[1] • Up to 140 Mbps of 3DES/AES-256 VPN throughput[1] using hardware acceleration (integrated in select models, optional for others) • VPN concentrator services (Easy VPN Server) for up to 2,000 remote users • Up to six 10/100 FE interfaces • VLAN trunking (802.1q tag-based) and OSPF dynamic routing support • Active/standby stateful failover support
PIX 525	• Enterprise-class integrated security appliance • Up to 330 Mbps of firewall throughput[1] • Up to 155 Mbps of 3DES/AES-256 VPN throughput[1] using hardware acceleration (integrated in select models, optional for others) • VPN concentrator services (Easy VPN Server) for up to 2,000 remote users • Gigabit Ethernet support; Up to eight 10/100 FE or three Gigabit Ethernet interfaces • VLAN trunking (802.1q tag-based) and OSPF dynamic routing support • Active/standby stateful failover support
PIX 535	• Carrier class large enterprise and service provider firewall appliance • Up to 1.7 Gbps of firewall throughput[1] • Up to 440 Mbps of 3DES/AES-256 VPN throughput using hardware acceleration (integrated in select models, optional for others) • VPN concentrator services (Easy VPN Server) for up to 2,000 remote users • Gigabit Ethernet throughput; Up to ten 10/100 FE or nine Gigabit Ethernet interfaces • VLAN trunking (802.1q tag-based) and OSPF dynamic routing support • Redundant, hot-swappable power supplies • Active/standby stateful failover support

[1] At 1400-byte packets

Key Features

- Security—Purpose-built firewall appliance with a proprietary, hardened operating system
- Performance—Stateful inspection firewall capable of up to 500,000 concurrent connections and 1.7 Gbps of throughput (at 1400-byte packets on Cisco PIX 535 Firewalls)
- High availability—Award-winning, active/standby stateful failover model provides enterprise-class, cost-effective resiliency
- Virtual Private Networking (VPN)—Supports both standards-based IPsec and L2TP/PPTP-based VPN services
- Optional PIX VPN Accelerator Card+—Scales 3DES/AES-256 VPN throughput up to 440 Mbps, using specialized co-processors designed for accelerating encryption operations
- Free software Cisco VPN Client provides secure connectivity across a broad range of platforms including Windows, Mac OS X, Linux and Solaris
- Network Address Translation (NAT) and Port Address Translation (PAT)—Conceals internal IP addresses and expands network address space
- Denial-of-Service (DoS) Attack Protection—Protects the firewall, internal servers and clients from disruptive hacking attempts
- OSPF dynamic routing support for improved network reliability and performance
- VLAN trunking (802.1q tag) support for simplified deployment in switched network environments
- Web-Based PIX Device Manager (PDM)—For simplified configuration and usage reports
- Auto Update, SSH, SNMP, TFTP, HTTPS, and telnet for remote management
- Support from two 10/100 Ethernet interfaces up to nine Gigabit Ethernet interfaces

Competitive Products

- Check Point Software: FireWall-1 / VPN-1
- NetScreen: NetScreen Security Appliances
- Nokia: IP-Series Security Appliances
- SonicWALL: SonicWALL Security Appliances
- WatchGuard Technologies: Firebox-series and V-series Security Appliances

Specifications

Feature	PIX 501	PIX 506E	PIX 515E	PIX 525	PIX 535
Processor	133 MHz	300 MHz	433 MHz	600 MHz	1.0 GHz
RAM	16 MB	32 MB	32 or 64 MB	128 or 256 MB	512 MB or 1 GB
Flash Memory	8 MB	8 MB	16 MB	16 MB	16 MB
PCI Slots	None	None	2	3	9
Fixed Interfaces (Physical)	Four port 10/100 switch (inside), One 10Base-T Ethernet (outside)	Two 10Base-T Ethernet	Two 10/100 Fast Ethernet	Two 10/100 Fast Ethernet	None
Maximum Interfaces (Physical and Virtual)	Four port 10/100 switch (inside), One 10Base-T Ethernet (outside)	Two 10Base-T Ethernet	Six 10/100 Fast Ethernet (FE) or 8 VLANs	Eight 10/100 FE or GEn or 10 VLANs	Ten-10/100 FE or GE or 24 VLANs
VPN Accelerator Card+ (VAC+) Option	No	No	Yes, integrated in select models	Yes, integrated in select models	Yes, integrated in select models
Failover Support	No	No	Yes, UR/FO models only	Yes, UR/FO models only	Yes, UR/FO models only
Size	Desktop	Desktop	1 RU	2 RU	3 RU

7665
6

Selected Part Numbers and Ordering Information[1]

Cisco PIX Bundles	
PIX-535-UR-BUN	PIX 535 Unrestricted Bundle (Chassis, unrestricted license, two 10/100 ports, VPN Accelerator Card+)
PIX-535-R-BUN	PIX 535 Restricted Bundle (Chassis, restricted license, two 10/100 ports)
PIX-535-FO-BUN	PIX 535 Failover Bundle (Chassis, failover license, two 10/100 ports, VPN Accelerator Card+)
PIX-525-UR-BUN	PIX 525 Unrestricted Bundle (Chassis, unrestricted software, two 10/100 ports, VPN Accelerator Card+)
PIX-525-R-BUN	PIX 525 Restricted Bundle (Chassis, restricted software, two 10/100 ports)
PIX-525-FO-BUN	PIX 525 Failover Bundle (Chassis, failover software, two 10/100 ports, VPN Accelerator Card+)
PIX-515E-UR-BUN	PIX 515E Unrestricted Bundle (Chassis, unrestricted software, two 10/100 ports, VPN Accelerator Card+)
PIX-515E-R-BUN	PIX 515E Restricted Bundle (Chassis, restricted software, two 10/100 ports)
PIX-515E-FO-BUN	PIX 515E Failover Bundle (Chassis, failover software, two 10/100 ports, VPN Accelerator Card+)
PIX-506E-506E-BUN-K9	PIX 506E 3DES/AES Bundle (Chassis, software, 3DES/AES license, two 10-BaseT ports)[2]
PIX-501-BUN-K8	PIX 501 10 User/DES Bundle (Chassis, SW, 10 user/DES licenses, 4 port 10/100 switch)
PIX-501-BUN-K9	PIX 501 10 User/3DES/AES Bundle (Chassis, SW, 10 user/3DES/AES licenses, 4 port 10/100 switch)[2]
PIX-501-50-BUN-K8	PIX 501 50 User/DES Bundle (Chassis, SW, 50 user/DES licenses, 4 port 10/100 switch)
PIX-501-50-BUN-K9	PIX 501 50 User/3ES/AES Bundle (Chassis, SW, 50 user/3DES/AES licenses, 4 port 10/100 switch)[2]
Cisco PIX Interfaces and Cards	
PIX-1GE-66	Single 66-MHz Gigabit Ethernet interface for PIX 53x (multimode fiber, SC connector)
PIX-1GE	Single Gigabit Ethernet Interface for PIX 52x
PIX-4FE	Four-port 10/100 Fast Ethernet interface
PIX-1FE	Single-port 10/100 Fast Ethernet interface
PIX-VPN-ACCEL	IPSec Hardware VPN Accelerator Card (VAC)
PIX-VPN-ACCEL-PLUS	PIX VPN Accelerator Card+ (VAC+)
Cisco PIX VPN Feature Licenses	
PIX-VPN-3DES	3DES/AES IPSec VPN software license for PIX 525/535[2]
PIX-515-VPN-3DES	3DES/AES IPsec VPN software license for PIX 515/515E[2]
PIX-506-SW-3DES	3DES/AES IPSec VPN software license for PIX 506/506E[2]
PIX-501-VPN-3DES	3DES/AES IPSec VPN software license for PIX 501[2]
PIX-VPN-DES	56-bit DES IPSec VPN software license
PIX Accessories	
PIX-506E-PWR-AC	Redundant AC power supply for PIX 506E
PIX-515-PWR-DC	Redundant DC power supply for PIX 515/515E

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

[2] AES encryption available with Cisco PIX Firewall Software version 6.3 and above.

For More Information

See the PIX Firewall Web site: **http://www.cisco.com/go/pix**

Cisco IOS Firewall

The Cisco IOS Firewall enriches Cisco IOS Software security capabilities, integrating robust firewall functionality and intrusion detection for every network perimeter. When combined with Cisco IOS IPSec software and other Cisco IOS Software-based technologies such as L2TP tunneling and quality of service (QoS), it provides a complete, integrated virtual private network solution. Because it is available for a wide range of Cisco routers, it gives customers the flexibility to choose a solution that meets their bandwidth, LAN/WAN density, and multiservice requirements, while benefiting from advanced security.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco IOS Firewall	• An integrated firewall solution with powerful security and multiprotocol routing all on the same platform • Scalability options from the Cisco 800 up to the Cisco 7500 and the Catalyst 6000 • Low cost solution where high performance is not a requirement • For secure extranet and intranet perimeters and Internet connectivity for branch and remote offices • Secure remote access or data transfer via a Cisco IOS Software-based VPN solution • Real-time (inline) integrated intrusion detection system (IDS) to complement firewall or existing IOS (Cisco Secure IDS) • Security and access to the network on a per-user basis

Key Features

- Context-based access control (CBAC) provides secure, stateful, application-based filtering, supporting the latest protocols and advanced applications
- Intrusion detection for real-time inline monitoring, interception, and response to network misuse
- Dynamic, per-user authentication/authorization for LAN, WAN, and VPN clients
- Graphical configuration and management via the ConfigMaker Security Wizard and Cisco Secure Policy Manager (CSPM)
- Provides strong perimeter security for a complete Cisco IOS Software-based VPN solution, including IPSec, QoS, and tunnelling for a wide range of Cisco routers

Competitive Products

- Lucent (Ascend): SecureAccess Firewall
- Nokia: IP400 Series
- Nortel: BaySecure Firewall-1
- Same competitors as PIX so they are also Checkpoint, Linksys, Nokia, Netscreen, etc.

Specifications

Feature	Cisco IOS Firewall
Supported Network Interfaces	All network interfaces on supported platforms
Supported Platforms	Cisco 1720, 2600/2600XM, 3600, 7100, and 7200 series router platforms (supports full feature set) Cisco 800, UBR900, 1600, and 2500 series router platforms include all firewall features with exception of intrusion detection and authentication proxy
Simultaneous Sessions	No maximum; dependent on platform, network connection, and traffic

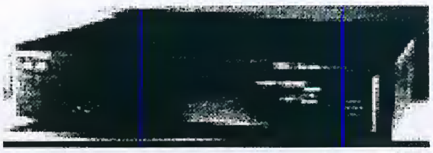
Part Numbers and Ordering Information

For Cisco IOS Images containing firewall (FW) and intrusion detection (IDS) capabilities, see individual product pages of supported platforms and the Cisco IOS Feature Navigator at http://www.cisco.com/go/fn (CCO login required) for part numbers and more info.

For More Information

See the Cisco IOS Firewall Feature Set Web site: **http://www.cisco.com/go/csis**

Cisco VPN 3000 Family



The Cisco VPN 3000 Concentrator Series—A family of purpose-built, remote access Virtual Private Network (VPN) platforms that incorporates high availability, high performance and scalability with the most advanced encryption and authentication techniques available today. Customers can greatly reduce costs by leveraging their ISPs' infrastructure and eliminate costly leased lines. This series supports small offices as well as large organizations with up to 10,000 simultaneous remote users per unit. With load balancing configured, multiple units can be clustered to enable unlimited remote access users. It also supports the widest range of VPN clients including Certicom MovianVPN client, Microsoft 2000 L2TP/IPsec Client, and Microsoft PPTP for Windows 95/98/ME/NT/2000/XP.

7663 5

The Cisco VPN 3002 Hardware Client—Combines the best capabilities of a software client with the reliability and stability of a dedicated hardware platform, and scales to tens of thousands of users. It sets up connections to a variety of Cisco VPN concentrators, including the VPN 3000 series and PIX firewalls.

When to Sell

Sell This Product	When a Customer Needs These Features
VPN 3005 and 3015 Concentrators	• A fixed configuration device designed for small- to medium-sized organizations with bandwidth requirements up to full-duplex T1/E1 (4 Mbps maximum performance) and up to 100 simultaneous remote access sessions • Encryption processing is performed in software • VPN 3015 is field-upgradable to the Cisco VPN 3030 and 3060 models and for redundancy
VPN 3030 and 3060 Concentrators	• VPN 3030 is for medium- to large-sized organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps max. performance) and up to 1500 simultaneous sessions; field-upgradeable to the Cisco VPN 3060 • VPN 3060 is for large organizations, with high-performance, high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps max. performance) and up to 5000 simultaneous remote access sessions • Both have specialized SEP modules to perform hardware-based acceleration
VPN 3080 Concentrator	• Optimized to support large enterprise organizations that demand the highest level of performance combined with support for up to 10,000 simultaneous remote access sessions • Specialized SEP modules perform hardware-based acceleration
VPN 3000 Client	• Establishes secure, end-to-end encrypted tunnels to the Cisco VPN 3000 Concentrator and other Cisco Easy VPN compliant devices. • Provided at no charge, installs on PCs and is available for Windows, MAC OS X and Linux/Solaris environments
VPN 3002 Hardware Client	• Emulates the software client in hardware • Ideal for mixed operating system environments and where corporation does not own/control remote PC or for very large applications requiring large number of devices due to ease of deployment, upgradability & scalability

Key Features

- Cisco VPN 3000 Concentrators Series
  - Support for industry standard IPSec DES/3DES/AES and Cisco IPSec/NAT for VPN Access through Port Address Translation firewalls
  - Unlimited-use license for Cisco VPN Client distribution included at no cost with multiple OS support including Windows, MAC OS X, Linux and Solaris; also integrates with Zone Alarms personal firewall
  - Supports standard authentication: RADIUS, SDI Tokens, and Digital Certificates
  - VPN load balancing allows for multiple units to cluster as a single shared pool
- Cisco VPN 3002 Hardware Client supports up to 253 users/stations per VPN 3002
  - Works with most operating systems including Windows, Linux, Solaris, and MAC OS X
  - Auto-upgrade capability automates upgrades with no user intervention required
  - Client technology employs push policy and automatic address assignment from the central site concentrator, enabling virtually unlimited scalability

Competitive Products

- Nortel: Contivity products
- Netscreen: LAN to LAN environments
- Nokia

Specifications

Cisco VPN 3000 Series Concentrators

Feature	VPN 3005	VPN 3015	VPN 3030	VPN 3060	VPN 3080
Simultaneous Users	100	100	1500	5000	10,000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	No	No	Optional	Optional	Yes
Expansion Slots	0	4	3	2	N/A
Upgradeable	No	Yes	Yes	N/A	N/A
Memory	32 MB	128 MB	128 MB	256 MB	256 MB
Hardware Configuration	1U, Fixed	2U, Scalable	2U, Scalable	2U, Scalable	2U
Power Supply	Single	Single, with a dual option	Single, with a dual option	Single, with a dual option	Dual
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
LAN-to-LAN Connections (internal user database)	100	100	500	1000	1000
Dimensions (HxWXD)	1.75 x 17.5 x 11.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.	3.5 x 17.5 x 14.5 in.

Cisco VPN 3002 Hardware Client

Feature	VPN 3002 Hardware Client
Hardware Processor	Motorola PowerPC processor; Dual flash image architecture
Network Interfaces	CPVN3002-K9: One Public 10/100Mbps RJ-45 Ethernet Interface and One Private Port 10/100Mbps RJ-45 Ethernet Interface CVPN3002-8E-K9: One Public 10/100Mbps RJ-45 Ethernet Interface and Eight Private Port 10/100Mbps RJ-45 Ethernet Interfaces via AUTO-MDIX switch
Physical Dimensions	1.967 x 8.6 x 6.5 in. (5 x 8.6 x 16.51 cm)
Power Supply	External AC Operation: 100-240V at 50/60 Hz with universal power factor correction; 4 foot cord included and international "pigtail" power cord selection
Tunneling Protocol Support	IPsec with IKE key management
Monitoring & Configuration	Event logging; SNMP MIB-II support Embedded management interface is accessible via console port or local web browser; SSH/SSL
Encryption Algorithms, Key Management & Authentication Algorithms	56-bit DES (IPsec); 168-bit Triple DES (IPsec); AES 128 & 256-bit (IPsec)
Authentication and Accounting Servers	Support for redundant external authentication servers including RADIUS Microsoft NT Domain authentication, X.509v3 Digital Certs (PKC7-PKCS10)
Configuration Modes	Client Mode—acts as client, receives random IP address from Concentrator Pool; Uses NAPT to hide stations 3002; Network behind 3002 is unroutable; few configuration parameters Network Extension Mode—acts as site-to-site device; Uses NAPT to hide stations only to Internet (stations visible to central site); Network behind 3002 is routable; additional configuration parameters

Selected Part Numbers and Ordering Information[1]

Cisco VPN 3000 Concentrator

CVPN3005-E/FE-BUN	CVPN3005-E/FE hw set, sw, client, & US power cord
CVPN3015-NR-BUN	CVPN3015-NR non-redundant hw set, sw, client, & US power cord
CVPN3030-NR-BUN	CVPN3030-NR non-redundant hw set, sw, client, & US power cord
CVPN3030-RED-BUN	CVPN3030-RED redundant hw set, sw, client, & US power cord
CVPN3060-NR-BUN	CVPN3060-NR non-redundant hw set, sw, client, & US power cord
CVPN3060-RED-BUN	CVPN3060-RED redundant hw set, sw, client, & US power cord
CVPN3080-RED-BUN	CVPN3080-RED redundant hw set, sw, client, & US power cord

Cisco VPN 3000 Series Upgrades

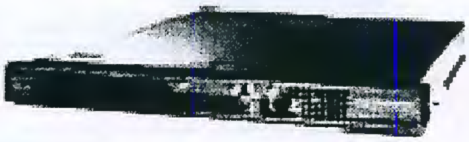
CVPN1530-UPG-RED	Cisco VPN 3015 To 3030 (Redundant) Upgrade Kit
CVPN1560-UPG-NR	Cisco VPN 3015 To 3060 (Non-Redundant) Upgrade Kit
CVPN1560-UPG-RED	Cisco VPN 3015 To 3060 (Redundant) Upgrade Kit
CVPN1580-UPG-RED	Cisco VPN 3015 To 3080 (Redundant) Upgrade Kit
CVPN3030-UPG-RED	Cisco VPN 3030 To 3080 (Redundant) Upgrade Kit
CVPN3060-UPG-NR	Cisco VPN 3030 To 3060 (Non-Redundant) Upgrade Kit

CVPN3080-UPG-R/R	Cisco VPN 3030 (Redundant) to 3080 (Redundant) Upgrade Kit
CVPN3080-UPG-RED	Cisco VPN 3030 To 3080 (Redundant) Upgrade Kit
CVPN3060-UPG-RED	Cisco VPN 3030 To 3060 (Redundant) Upgrade Kit
CVPN6060-UPG-RED	Cisco VPN 3060 To 3060 (Redundant) Upgrade Kit
CVPN6080-UPG-RED	Cisco VPN 3060 To 3080 (Redundant) Upgrade Kit
CVPN3060-UPG-R/R	Cisco VPN 3030 (Redundant) to 3060 (Redundant) Upgrade Kit
CVPN6080-UPG-R/R	Cisco VPN 3060 (Redundant) to 3080 (Redundant) Upgrade Kit
Cisco VPN 3000 Series Accessories	
CVPN3000-PWR=	Cisco VPN 3000 Concentrator Power Supply
Cisco VPN 3000 Series Basic Maintenance	
CON-SNT-PKG4	SMARTnet Maintenance for Cisco CVPN3005-E/FE-BUN
CON-SNT-PKG8	SMARTnet Maintenance for Cisco CVPN3015-NR-BUN
CON-SNT-PKG11	SMARTnet Maintenance for Cisco CVPN3030-NR-BUN
CON-SNT-PKG13	SMARTnet Maintenance for Cisco CVPN3030-RED-BUN
CON-SNT-PKG14	SMARTnet Maintenance for Cisco CVPN3060-RED-BUN
Cisco VPN Client	
CVPN-CLIENT-K9=	Cisco VPN Client CD (included with Concentrator purchase)

For More Information

See the Cisco VPN 3000 series Web site: **http://www.cisco.com/go/vpn3000**

Cisco Intrusion Detection System Network Sensors



Cisco integrated network security solutions enable organizations to protect productivity gains and reduce operating costs. The Cisco Intrusion Protection is designed to efficiently protect your data and information infrastructure. Cisco delivers four four critical elements for efficient intrusion protection system which are:

- Accurate threat detection—Cisco Intrusion Detection System Version 4.0 (Cisco IDS 4.0) delivers the first step in providing a secure environment by comprehensively detecting all potential threats
- Intelligent threat investigation—Cisco Threat Response technology virtually eliminates false alarms, and automatically determines which threats need immediate attention to avoid costly intrusions.
- Ease of management—Browser-based tools simplify the user interaction, while providing powerful analytical tools that allow for a rapid and efficient response to threats.
- Flexible deployment options—A range of high-availability devices provide the flexible backbone for creating the secure and efficient intrusion protection system.

The current Cisco IDS sensing portfolio includes the following sensor appliances: IDS 4210, IDS 4235, IDS 4250, and IDS 4250-XL. Additionally, Cisco IDS delivers network protecting that is integrated into the Catalyst 6500 switch with the Intrusion Detection System Module (IDSM-2).

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco IDS Network Sensors	• Cisco network IDS appliances are network-based, real-time intrusion detection systems capable of monitoring an entire enterprise network • Performance requirements from 45 Mbps to 1 Gbps • The Cisco IDS Module enables customers to perform both security monitoring and switching functions within the same chassis • A robust, 24 hour x 7 day-a-week monitoring and response system with the latest attack detection capabilities • A distributed intrusion detection system capable of directing and forwarding alarms between local, regional, and headquarters-based monitoring consoles • A scalable architecture to allow the deployment of large numbers of sensors in order to provide comprehensive security coverage in large network environments. • An intrusion detection system designed to integrate smoothly with existing network management tools and practices • Automated false alarm reduction capabilities • Integration of full featured IDS protection into the Cisco Catalyst 6500 chassis

Key Features

- High-Speed Performance including support for full line rate gigabit environments
- Easy Installation and Setup; Remote Configuration Capability
- Fault-Tolerant Communications
- Comprehensive Attack Database
- Custom User-Defined Signatures; Automatic Signature Updates
- Notification actions
- Ability to Monitor 802.1q (trunked) traffic
- Secure web-based embedded device management and event monitoring
- Comprehensive IDS Anti-Evasion Techniques
- Cisco IOS-like CLI for full featured IDS management capabilities

Competitive Products

- Internet Security Systems (ISS): RealSecure
- Symantec: Recourse Manhunt & ManTrap/NetProwler
- Enterasys: Dragon IDS
- Intrusion.com: SecureNet
- Snort: IDS
- Tipping Point
- nCircle
- Network Flight Recorder, Inc.: NFR

Specifications

Feature	IDS-4210	IDS-4235	IDS-4250	IDS-4250-XL	IDS Module (IDSM-2)
Performance	45 Mbps	200 Mbps	500 Mbps	1000 Mbps	600 Mbps
Processor	566 MHz	1.26 GHz	Dual 1.26 GHz	Dual 1.26 GHz. Includes customized HW acceleration	Custom Hardware
RAM	256 MB	1 GB	2 GB	2 GB	
Network Interface Card	Autosensing 10/100 Base-T Ethernet	Autosensing 10/100/1000 Base-T Ethernet	Autosensing 10/100/1000BASE-TX with optional 1000-Base SX (fiber)	Dual 1000BASE-SX interface with MTRJ	PCI
Command & Control Interface	Autosensing 10/100 Base-T Ethernet	Autosensing 10/100/1000Base-TX	Autosensing 10/100/1000Base-TX	Autosensing 10/100/1000Base-TX	PCI

Selected Part Numbers and Ordering Information[1]

Cisco IDS Network Appliance Sensor

IDS-4210-K9	4210 Sensor (Chassis, s/w, two 10/100 ports, up to 45Mbps)
IDS-4235-K9	Cisco IDS 4235 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector, up to 200 Mbps)
IDS-4250-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector, upto 500 Mbps)
IDS-4250-XL-K9	Cisco IDS 4250-XL Sensor (chassis, software, SSH, hardware accelerator with dual 1000BASE-SX and MTRJ connectors)

Cisco IDS Switch Sensor Options

WS-SVC-IDS2-BUN-K9	Intrusion Detection System Module for Catalyst 6K Switch (IDSM-2)

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

Note **Export Considerations:** The Cisco IDS 4210, Cisco IDS 4235, Cisco IDS 4250, Cisco IDS 4250-XL and Cisco IDSM-2 are subject to export controls. Please refer to the export compliance Web site at **http://www.cisco.com/wwl/export/crypto** for guidance. For specific export questions, please contact **export@cisco.com**.

For More Information

See the Cisco IDS Web site: **http://www.cisco.com/go/ids**

Cisco Security Agent

The next-generation Cisco Security Agent network security software provides threat protection for server and desktop computing systems, also known as "endpoints." The Cisco Security Agent goes beyond conventional host and desktop security solutions by identifying and preventing malicious behavior before it can occur, thereby removing potential known and unknown ("Day Zero") security risks that threaten enterprise networks and applications. The Cisco Security Agent aggregates and extends multiple endpoint security functions by providing host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent package.

The Cisco Security Agent analyzes behavior rather than relying on signature matching, its solution provides robust protection with reduced operational costs. Customers require robust endpoint security that prevents security attacks from affecting the network and critical applications.

As a key component of the SAFE blueprint for secure e-business, the Cisco Security Agent provides unprecedented endpoint protection that enables businesses to participate in e-commerce securely and take advantage of the Internet economy.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Security Agent	• Host intrusion protection, distributed firewall, malicious mobile code protection, operating system hardening, file integrity and/or audit log consolidation. The Cisco Security Agent provides all of these features in one integrated package • Protection against both known and unknown attacks • Protection for servers and/or desktops/laptops • A solution that is scalable to protect thousands of servers and desktops for large enterprise deployments

Key Features

- Provides industry-leading protection for Unix and Windows servers
- Open, extensible architecture offers the capability to define and enforce security according to corporate policy

Competitive Products

- Internet Security Systems (ISS)
- Symantec: Intruder Alert
- Enterasys: Squire
- Entercept
- NFR (Centrax)

Specifications

Feature	Cisco Security Server Agent	Cisco Security Desktop Agent	Cisco Security Agent Manager
Platforms	Windows 2000 Server and Advanced Server (up to Service Pack 3)	Windows NT v4.0 Workstation (Service Pack 5 or later)	Microsoft Windows 2000 Server and Advanced Server (up to SP 2)
	Windows NT v4.0 Server and Enterprise Server (Service Pack 5 or later)	Windows 2000 Professional (up to Service Pack 3)	
	Solaris 8 SPARC architecture (64-bit kernel)	Windows XP Professional (up to Service 1)	

Selected Part Numbers and Ordering Information[1]

Cisco Security Agent Options	
CSA-MANAGER-K9	Cisco Security Agent Manager (CD Kit)
CSA-SRVR-K9=	Cisco Security Server Agent (Win & Sol), 1 Agent
CSA-B10-SRVR-K9	Cisco Security Server Agent (Win & Sol), 10 Agent Bundle
CSA-B25-DTOP-K9	Cisco Security Desktop Agent, 25 Agent Bundle
CSA-B100-DTOP-K9	Cisco Security Desktop Agent, 100 Agent Bundle

Note **Export Considerations:** The Cisco Security Agent is subject to export controls. Please refer to the export compliance Web site at **http://www.cisco.com/wwl/export/crypto** for guidance. For specific export questions, please contact **export@cisco.com**.

For More Information

See the Cisco Security Agent Web site: **http://www.cisco.com/go/securityagent**

Cisco 7100 Series

The Cisco 7100 series VPN router is a high-end, integrated VPN solution that melds high-speed, industry-leading routing with a comprehensive suite of advanced site-to-site VPN services. The Cisco 7100 series VPN router integrates key features of VPNs—tunneling, data encryption, security, firewall, advanced bandwidth management, and service-level validation—to deliver self-healing, self-defending, VPN platforms that cost-effectively accommodatc remote-office and extranet connectivity using public data networks. The Cisco 7100 series VPN router offers specific hardware configurations optimized for VPN applications and network topologies. Optional WAN and embedded Fast Ethernet interfaces combined with high-performance routing and rich VPN services provide turnkey VPN routing solutions.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco 7120	• Entry-level Cisco 7100 Series Router designed for large branch or central site VPN with VPN services throughput of up to 50 Mbps • Designed primarily for site-to-site VPN deployments with incidental remote access requirements
Cisco 7140	• High-end site-to-site VPN platform for central site VPN applications with VPN services throughput up to 140 Mbps • Provides superior routing and VPN services performance for central site environments, as well as dual power supplies for increased solution reliability

7657 3

Key Features

- Comprehensive suite of VPN services—tunneling, data encryption, security, firewall, quality of service, and service level validation—integrated with industry leading routing
- High performance RISC processor delivering high-speed, scalable VPN services and routing throughput and extensive memory for reliable, high-speed VPN services delivery
- Dual autosensing 10/100BASE-T Fast Ethernet ports for connectivity to the corporate LAN; the Cisco 7120 Series also has an integrated 4-port T1/E1 serial WAN interface
- Integrated Services Module (ISM) is included for support up to 2000 simultaneous tunneling sessions with 90 Mbps encryption performance and Windows 95/98/NT4.0 and Windows 2000 compatibility for remote access; an optional Integrated Services Adapter (ISA) may be installed in the Cisco 7140 to provide dual encryption acceleration performance up to 3000 tunnels and 140 Mbps 3DES encryption throughput

Competitive Products

- Check Point: VPN-1 Appliance
- Nortel: Contivity 4500
- Nokia: IP440

Specifications

Feature	Cisco 7120	Cisco 7140
Embedded Dual 10/100BASE-T Fast Ethernet Interfaces	Autosensing, RJ-45	Autosensing, RJ-45
WAN Physical Interfaces	EIA/TIA-232, EIA/TIA-449, X.21, V.35, EIA-530	None
WAN/LAN Interface Expansion Slot	1 slot	1 slot
Supported Network and Services Port Adapters	Gigabit Ethernet 1000BASE-SX and 1000BASE-LX/LH Fast Ethernet 100BASE-TX and 100BASE-FX Fast Ethernet/ISL TX and ISL FX Ethernet 10BASE-T and 10BASE-FL Dedicated Token Ring Multichannel T1 and E1 ATM Synchronous Serial HSSI ISDN BRI Packet over SONET OS3/STM1 Integrated Services Adapter (ISA)	Same as Cisco 7120
Service Module Slot	1 slot	1 slot
Included Service Modules	Integrated Services Module (ISM)	Integrated Services Module (ISM)
Console and Auxiliary Ports	1 of each, RJ-45 interface	1 of each, RJ-45 interface
SDRAM	64 MB packet 128 MB system (expandable to 256 MB)	64 MB packet 128 MB system (expandable to 256 MB)
Flash Memory	48 MB	48 MB
PCMCIA Slots for Flash Memory	2	2
Power Supply	Single AC	Dual AC
Dimensions (HxWxD)	3.5 in. x 17.5 in. x 18.25 in.	3.5 in. x 17.5 in. x 18.25 in.

Cisco IOS Software and Memory Requirements[1]

To run the Cisco IOS Software Feature Packs, you need, at a minimum, the amount of memory shown in the following table. Some configurations will require more than the recommended minimum.

Distribution Part Number	Feature Pack Description	IOS Image Release	Flash Memory Required	DRAM Memory Required
CD71-CL-12.1.6E=	IP IPSEC 56	12.1(6)E	16MB	64MB
CD71-CK2-12.1.6E=	IP IPSEC 3DES	12.1(6)E	16MB	64MB
CD71-CHK2-12.1.6E=	IP/FW/IDS IPSEC 3DES	12.1(6)E	16MB	64MB
CD71-AL-12.1.6E=	Enterprise IPSEC 56	12.1(6)E	16MB	64MB
CD71-AK2-12.1.6E=	Enterprise IPSEC 3DES	12.1(6)E	16MB	64MB
CD71-AHK2-12.1.6E=	Enterprise/FW/IDS IPSEC 3DES	12.1(6)E	16MB	64MB

[1] For the complete list of IOS Feature Sets, refer to the parts list, via the URL listed under "For More Information". For users with CCO access, search by IOS feature or release via the *Feature Navigator* at http://www.cisco.com/go/fn

Selected Part Numbers and Ordering Information[1]

Cisco 7100 Series Bundles—7120	
CISCO7120-4T1/VPN	7120-4T1 VPN Bundle, ISM, 2xFE, AC PS, IPSEC DES
C7120-4T1/VPN/K9	7120-4T1 VPN Bundle, ISM, 2xFE, AC PS, IPSEC 3DES
Cisco 7100 Series Bundles—7140	
CISCO7140-2FE/VPN	7140-2FE VPN Bundle, ISM, 2xFE, 2xAC PS, IPSEC DES
C7140-2FE/2VPN/K8	7140-2FE VPN Bundle, ISM & ISA, 2xFE, 2xAC PS, IPSEC DES
C7140-2FE/2VPN/K9	7140-2FE VPN Bundle, ISM & ISA, 2xFE, 2xAC PS, IPSEC 3DES
C7140-2FE/VPN/K9	7140-2FE VPN Bundle, ISM, 2xFE, 2xAC PS, IPSEC 3DES
Cisco 7100 Port Adapters	
PA-FE-TX	1-port Fast Ethernet 100BaseTx Port Adapter
PA-FE-FX	1-port Fast Ethernet 100BaseFx Port Adapter
PA-2FE-TX	2-port Fast Ethernet 100BaseTx Port Adapter
PA-2FE-FX	2-port Fast Ethernet 100BaseFx Port Adapter
PA-2FEISL-TX	2-port Token Ring ISL 100BaseTx Port Adapter
PA-2FEISL-FX	2-port Token Ring ISL 100BaseFx Port Adapter
PA-4E	4-port Ethernet 10BaseT Port Adapter
PA-8E	8-port Ethernet 10BaseT Port Adapter
PA-5EFL	5-port Ethernet 10BaseFL Port Adapter
PA-4T+	4-port Serial Port Adapter, Enhanced
PA-8T-V35	8-port Serial, V.35 Port Adapter
PA-8T-232	8-port Serial, 232 Port Adapter
PA-8T-X21	8-port Serial, X.21 Port Adapter
PA-4R-DTR	4-port Dedicated Token Ring, 4/16Mbps, HDX/FDX Port Adapter
PA-GE	Gigabit Ethernet Port Adapter
PA-H	1-port HSSI Port Adapter
PA-2H	2-port HSSI Port Adapter
PA-A3-T3	1-port ATM Enhanced DS3 Port Adapter
PA-A3-E3	1-port ATM Enhanced E3 Port Adapter
PA-A3-OC3MM	1-port ATM Enhanced OC3c/STM1 Multimode Port Adapter
PA-A3-OC3SMI	1-port ATM Enhanced OC3c/STM1 Single mode (IR) Port Adapter
PA-A3-OC3SML	1-port ATM Enhanced OC3c/STM1 Single mode (LR) Port Adapter
PA-4E1G/75	4-port E1 G.703 Serial Port Adapter (75ohm/Unbalanced)
PA-4E1G/120	4-port E1 G.703 Serial Port Adapter (120ohm/Balanced)
PA-E3	1-port E3 Serial Port Adapter with E3 DSU
PA-2E3	2-port E3 Serial Port Adapter with E3 DSUs
PA-T3	1-port T3 Serial Port Adapter with T3 DSUs
PA-2T3	2-port T3 Serial Port Adapter with T3 DSUs
PA-MC-2T1	2-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-2E1/120	2-port multichannel E1 port adapter with G.703 120ohm interf
PA-MC-4T1	4-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-8T1	8-port multichannel T1 port adapter with integrated CSU/DSUs
PA-MC-8E1/120	8-port multichannel E1 port adapter with G.703 120ohm interf
PA-POS-OC3MM	1-port Packet/SONET OC3c/STM1 Multimode Port Adapter
PA-POS-OC3SMI	1-port Packet/SONET OC3c/STM1 Single mode (IR) Port Adapter
PA-POS-OC3SML	1-port Packet/SONET OC3c/STM1 Single mode (LR) Port Adapter
SM-ISM	Integrated Services Module for IPSec & MPPE encryption
SA-ISA	Integrated Services Adapter for IPSec or MPPE encryption

PA-4B-U	4-port BRI Port Adapter, U Interface
PA-8B-S/T	8-port BRI Port Adapter, S/T Interface

1. This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco 7100 series Web site: **http://www.cisco.com/go/7100**

Cisco Secure Access Control Server for Windows

Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) server system. Cisco Secure ACS controls the authentication, authorization, and accounting (AAA) of users and administrators accessing corporate resources through the network. Cisco Secure ACS greatly reduces the administrative and management burden involved in scaling user and network administrative access to your network. Cisco Secure ACS centralizes the administration of user access controls globally to ensure enforcement of assigned policies.

ACS 3.1 provides support for the latest security architecture for Wireless authentication. It also includes SSL server authentication and encryption for administrative login.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Secure Access Control Server (ACS) for Windows	• Centrally manage who can log in to the network from wired or wireless connections • Privileges each user has in the network • Accounting information recorded in terms of security audits or account billing • What access and command controls are enabled for each configuration administrator • Virtual VSA for Aironet rekey • Secure server authentication and encryption • Simplified firewall access and control through Dynamic Port Assignment • Same User AAA services

Key Features

- PEAP support—Provides a new, secure client-server authentication method for wireless networks; Provides new support for one-time token authentication, password change/aging and powerful extensibility of end-user databases such as LDAP, NDS, and ODBC.
- SSL support for administrative access—Administrative access via the Web GUI can be secured with SSL, both certificate-based and encrypted tunnel support
- CHPASS improvements—Allows privileged users control over whether network administrators can change passwords during TACACS+ AAA client-hosted Telnet sessions
- Improved IP pool addressing mechanism—Includes a new, efficient algorithm for allocating IP addresses
- Device search mechanism—Allows users to search for a configured AAA device based on the device name, IP address, type (RADIUS or TACACS+), or device group
- Improved PKI support—Provides a more secure PKI authentication scheme by verifying the user's certificate authority stored in the remote LDAP directory against the one provided by the client

- EAP proxy enhancements—Extends EAP (LEAP, PEAP, or EAP-transport layer security [TLS]) proxy to other RADIUS or external databases using standard RADIUS proxy
- Integration with Cisco's security management software applications—Provides a consolidated administrative TACACS+ control framework for many Cisco security management tools such as CiscoWorks VPN/Security Management Solution (VMS)

Competitive Products

- Funk: Steel Belted RADIUS
- Lucent/Avaya: Security Management Server (LSMS)
- Nortel: Preside RADIUS Server (OEM of Funk product)

Specifications

Feature	Cisco Secure Access Control Server (ACS) for Windows
Platform	Windows 2000 Server must meet the following minimum hardware requirements:Pentium processor, 550 MHz or faster; Minimum resolution of 256 colors at 800 x 600 lines
RAM	256 MB required; more if you are running your database on the same machine
Disk Drive	250 MB of disk space; more if you are running yoru database on the same machine
Software Requirements[1]	Cisco Secure ACS Server uses an English-language version of Windows 2000 Server. For specific types of service packs supported, refer to online documentation.The Windows server that runs Cisco Secure ACS must have a compatible browser installed. Cisco Secure ACS was tested with English-language versions of the following browsers on Microsoft Windows operating systems: Microsoft Internet Explorer 5.5 and 6.0, Netscape Communicator 6.2
Platform Requirements	Cisco IOS Software 11.2 or higher on Cisco Routing Solutions

[1] Beginning with Cisco Secure ACS Version 3.1, Cisco Secure ACS on a Windows NT 4.0 server is no longer supported. For information about upgrading the operating system of a server running Cisco Secure ACS, see the Installation Guide for Cisco Secure ACS for Windows Server, Version 3.1

Selected Part Numbers and Ordering Information[1]

Cisco Secure Access Control Server (ACS) for Windows

CSACS-3.1-WIN-K9	Cisco Secure ACS 3.1 for Windows
CSACS-3.1-WINUP-K9	Upgrade to CSACS 3.1 for Windows from ACS versions 1.x, 2.x, 3.0 and Cisco Secure ACS for Unix version 2.x

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Secure ACS for Windows Web site: **http://www.cisco.com/go/acs**

Cisco Secure User Registration Tool

Cisco Secure URT is a virtual LAN (VLAN) assignment service that provides LAN security by actively identifying and authenticating users and then associating them only to the specific network services and resources they need through dynamic VLAN assignments to Cisco Catalyst® Switch networks. URT v2.5 introduces many innovative features, including a Web-based logon from Windows, Macintosh, and Linux clients, RADIUS and Lightweight Directory Access Protocol (LDAP) authentication, and a secure link between the client and the VLAN Policy Server (VPS). It also includes a security feature based on the Media Access Control (MAC) address that prevents users from accessing the network if they are not using authorized machines. Web based LAN authentication allows for user mobility within the LAN environment.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Secure User Registration Tool (URT)	• Web-based LAN authentication for Windows, Macintosh, and Linux client platforms—ideal for mobile users within the LAN environment • Extended security to protect user access to the logon VLAN from unregistered PCs through MAC-based security option • RADIUS authentication and accounting support • Multiple user access per port

Key Features

- Web Client Logon Interface—Supports customizable Web-based authentication for Windows, Macintosh, and Linux client platforms
- MAC-Based Security Option—Provides extended security to protect user access to the logon VLAN from unregistered PCs
- RADIUS Authentication and Accounting Support—RADIUS authentication is offered for Web logon
- Secure Link Between Cisco Secure URT Client and VPS Server—Security authentication and data encryption have been added to URT v2.5 to enable a more secure connection from the user
- LDAP Support (Active Directory and NDS directories)—Cisco Secure URT v2.5 supports Windows' Active Directory and Novell's NDS LDAP servers
- Multiple Users Per Port—Previous versions of Cisco Secure URT support only a single user logon on a single port
- Display of Windows NT Groups—The URT Administrator interface is enhanced to display the users belonging to a Windows NT group
- MAC Address Events History—With URT v2.5 MAC-address-based logon/logoff events are added as an option and reported to the history events tool

Specifications

Feature	Cisco Secure User Registration Tool (URT)
Server Requirements	Windows 2000 (SP2) server, professional, and Windows XP Professional-Min H/W (Pentium III, 512MB DRAM, 65 MB of disk space)
Browser for Web Login	Netscape version 4.79 and 6.2; IE version 5.5 (SP2) or 6.0
Client Software Requirements	Windows 98 (2ndE), Windows NT4 Workstation/Server (SP6A), Windows 2000 (SP2) Professional/server, Windows XP Professional, Windows XP Home (Web Client Only), Mac OS 10.1 (Web client only), Linux Redhat/ SuSE/ Mandrake/ VA (Web Client only)-Min H/W for Web client (Pentium II, 256MB DRAM, 65 MB of disk space), Min H/W for traditional client (Pentium II, 64MB DRAM, 1MB of disk space)
Supported Cisco Products (latest tested version)	1900 series (1912, 1924), v9.00.05; C2800 series (2822, 2828), v9.00.05; C2900XL series (2908XL, 2916XL, 2912XL, 2912LRE-XL, 2924XL, 2924LRE-XL), v12.0(5)WC3b; C2948GL3 series (2948GL3, 4232) v12.0(18)W5(22b); C2950 series, v12.1.6.EA2c; C3500XL series (3508XL, 3512XL, 3524XL, 3548XL, 3550XL), v12.0(5)WC3b; C3550 series, v12.1.8.EA1c; C4000 series (4003, 4006, 4912g), v7.1(2); C5000 series (2900, 2926, 2948, 5000, 5002, 5500, 5505, 5509), v6.3(5); C6000 series (6006, 6009, 6506, 6509, 6513), v7.1(3)

Selected Part Numbers and Ordering Information[1]

Cisco Secure User Registration Tool (URT)

URT-2.5-K9	Starter Kit: includes one (1) User Registration Tool 2.5 Software license, and one (1) Cisco 1101 VLAN Policy Server (VPS) appliance
URT-2.5-UP	Software only; upgrades customers from URT 2.X to 2.5; includes upgrade for both URT Admin Server and Cisco 1100 VPS appliance
URT-1101-HW-K9	Hardware Only; Cisco 1101 VPS appliance; additional appliance needed for backup, use in distributed deployments, or deployments requiring Web logon capabilities

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco Secure User Registration Tool Web site: **http://www.cisco.com/go/urt**

CHAPTER 6

Content Networking Products

Content Networking Products at a Glance

Product	Features	Page
Cisco Content Engine 500 Series	Content services edge delivery platform for Enterprise networks • Functions as edge node device in an Application and Content Networking (ACN) system • Responsible for delivery of cached or distributed content to the end-user • Enables customers to rapidly deliver strategic applications to branch personnel including web application and content acceleration, content filtering and business video • Lays the foundation for advanced services such as e-learning and point of sale video delivery.	6-2
Cisco Content Engine 7300 Series	Content services platform for Enterprise data center and Service Provider networks • Offers premium hosting services • Caching capabilities optimize Web site performance and WAN bandwidth utilization • Offers transparent and Internet proxy caching, Content Filtering and ECDN capabilities in a single platform • Accelerates both HTTP and streaming media file formats	6-2
Content Engine Network Modules	Content services edge delivery network module for 2600, 3600, 3700 branch routers • Functions as edge node device in an Application and Content Networking (ACN) system • Enables delivery of new applications and services via a Cisco branch router with no performance degradation of core routing services • Allows rapid delivery of strategic applications to branch personnel including web application and content acceleration, content filtering and business video	6-2
Cisco 11500 Series Content Services Switches	Next-generation intelligent platform for Web site and e-commerce optimization • Provides an intelligent, distributed architecture to scale for today's e-business infrastructure • Offers Adaptive Session Redundancy (ASR)—a new industry standard in stateful failover • Delivers the greatest flexibility of any content switch in its class for customizing combinations of ports, performance, and services	6-4
Cisco LocalDirector	Integrated hardware and software solution for load balancing across servers • Allows many servers to appear as one server for high availability and easy scalability • Secure real-time embedded operating system	6-6
Cisco Content Distribution Manager 4600 Series	Content networking policy and management device • Central control over acquisition and distribution of content, including live and video on demand video, over IP networks • Intuitive web-based GUI provides integrated, easy-to-use management over caching and content delivery functions such as multicast replication, intelligent cache bypass and bandwidth management • Roles based access control securely enables multiple administrators and content publishers across the organization	6-7
Cisco Content Router 4430	Integrated global load balancing solution for content delivery networks • Solves distributed server site selection problems • Uses HTTP (CR-4430) to redirect a client to the best site on the Internet based on network delay • Transparently redirection redirects end user requests to the end user and works with any IP application • Extremely fast site-selection algorithm is optimized for high performance Web-style transactions	6-9
Content Switching Module (CSM) for the Catalyst 6500 Series Switches	Line card for Catalyst 6500 • Balances client traffic across multiple servers within server farms • URL and Cookie-based load balancing • High-performance—200,000 new Layer 4 TCP connection setups per second	6-11
Cisco SSL Module for Catalyst 6500	• Offloads SSL encryption and decryption • Scalable performance • Stickyness	6-11

Product	Features	Page
Cisco 11000 Series Secure Content Accelerator (SCA 11000)	Appliance-based SSL solution • Offloads SSL encryption/decryption from Web servers • Supports 200 new SSL connections and 900 sustained SSL sessions per second • Interoperates with the CSS 11000 for intelligent load balancing of SSL traffic	6-12
Cisco CTE-1400 Series Content Transformation Engine	Transforms Web and XML-based applications for display and interaction on IP Telephones, PDAs, WAP Phones and other non PC devices • Supports a broad range of end devices • Transforms existing applications • Design Studio GUI Application	6-13
Cisco DistributedDirector	Global Internet service scaling solution • Solves distributed server site selection problems. Enables a set of distributed servers to be seen as a single virtual server • Uses DNS to redirect a client to the best site on the Internet based on a variety of options • Configurable as authoritative Domain Name Services (DNS) caching name server and/or HTTP Session Redirector on a per-domain basis	6-14
Cisco GSS 4480 Global Site Selector	Global site selection for distributed data centers • Delivers global load balancing for multiple data centers • Offloads Domain Named System (DNS) servers by doing DNS resolution • Scales to support hundreds of data centers or server load balancers (SLBs)	6-15

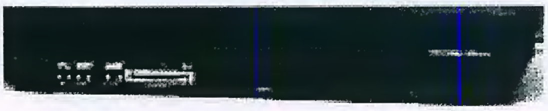
Content Networking Overview

Cisco Content Networking solutions are designed to optimize the delivery of content to end users. To accomplish this, Cisco offers solutions for both data center and edge delivery with industry-leading products in both categories.

In the data center, Cisco Content Switching, or L4-7 Switching, solutions optimize any size network to dynamically enable faster responses to Web requests and decrease network bandwidth congestion. Content switching, or intelligent load balancing, insures high levels of content availability and security, and leverages investment in Cisco IP infrastructure.

Cisco's Application and Content Networking (ACN) System allows enterprises to accelerate mission critical web applications such as Siebel and SAP, block viruses and inappropriate web sites and deliver business video, while laying the foundation for advanced services such as e-learning and point of sale video delivery. For Service Providers, the Cisco ACN System represents a highly profitable, new revenue opportunity by enhancing the customer/user Web experience and significantly accelerating the delivery of rich Web applications, content and streaming media.

Cisco Content Engines



Within Cisco's content-networking solutions portfolio, the Cisco Application and Content Networking System (ACNS) Software enables a variety of services that optimize delivery of Web applications and content from the network edge to ensure enhanced speed, availability, and performance for users. ACNS Software combines the technologies of transparent caching and enterprise content-delivery network (ECDN) for accelerated delivery of Web objects, files, and streaming media from a single intelligent edge appliance, the Cisco Content Engine (CE).

The Cisco ECDN solution provides a platform that delivers immediate benefits from entry-level applications such as content and business application acceleration and URL filtering, while laying the foundation for advanced services such as business video and e-learning.

When to Sell

Sell This Product	When a Customer Needs These Features
Content Engine 7325	• Ultra high-end content delivery capabilities for advanced applications such as streaming media, e-learning, and corporate communications
Content Engine 7305	• High-end content delivery capabilities for advanced applications such as streaming media, e-learning, and corporate communications
Content Engine 565	• Mid-range branch office and datacenter cache ideal for transparent caching, URL filtering, and edge content delivery
Content Engine 510	• Entry-level transparent caching and URL filtering capabilities along with limited content delivery
Content Engine Network Modules	• Router-integrated caching and content delivery network modules for 2600, 3600, 3700 branch access routers

Key Features

- Caching—Provides accelerated content delivery, WAN bandwidth cost savings, and protection vs. uncontrollable bottlenecks
- Content Filtering—Enables administrators to block, monitor, and report on end users' access to non-business and objectionable content (uses N2H2 Internet Filtering Protocol, Secure Computing SmartFilter, or Websense Enterprise Software)
- Content Delivery—Use in conjunction with Cisco Content Distribution Manager to enable rich media e-learning and corporate communications; deliver new premium hosting services such as on-demand content delivery and streaming media; and, to scale Web sites

Competitive Products

- Blue Coat: Blue Coat Server Accelerator 700 and 7000 Series and Blue Coat Systems Director
- Volera: Excelerator, Media Excelerator, Secure Excelerator
- Network Appliance: NetCache C1200/2100/6100 Series Appliances and Content Director

Specifications

Feature	Cisco Content Engine 7325	Cisco Content Engine 7305	Cisco Content Engine 565	Cisco Content Engine 510	Cisco CE Network Module	Cisco SA-7 and SA-14
Supported Interfaces	Two 10/100/1000BASE-TX	Two 10/100/1000BASE-TX	Two 10/100/1000BASE-TX	Two 10/100/1000BASE-TX	One internal 10/100-Mbps Ethernet to router backplane; one external 10/100-Mbps Ethernet	
SDRAM	4 GB	2 GB	1 GB	512 MB	Up to 512 MB	
Max Storage	936 GB	936 GB	396 GB	80 GB	396 GB	252 or 540 GB
	Ultra2 SCSI	Ultra2 SCSI	Ultra2 SCSI	IDE	Ultra2 SCSI	Ultra2 SCSI
Maximum Internal Storage	432 GB	432 GB	72 GB	80 GB	20 GB or 40 GB	252 or 540 GB
	Ultra2 SCSI	Ultra2 SCSI	Ultra2 SCSCO	IDE	IDE	Ultra2 SCSI
Flash Memory	128 MB	128 MB	128 MB	128 MB	16 MB internal; optional Compact Flash Memory	
Storage Array Support	Yes	Yes	Yes	No	Yes	
Rack Units	2 RU	2 RU	1 RU	1 RU	N/A	3 RU
Dimensions (HxWXD)	3.36 x 17.46 x 27.48 in	3.36 x 17.46 x 27.48 in.	1.72 x 17.3 x 16.75 in.	1.72 x 17.3 x 16.75 in.	One slot in 2600/3600/3700 chassis	5.0 x 17.5 x 20.4 in
Weight	62 lb.	62 lb.	28 lb.	28 lb.	1.5 lb.	76 lb.
Power	Hot-swappable redundant AC (DC availabled mid-2003)	Hot-swappable redundant AC (DC availabled mid-2003)	200W AC	200W AC	From 2600/3600/3700 chassis	AC (DC available mid-2003)

7649
3

Selected Part Numbers and Ordering Information[1]

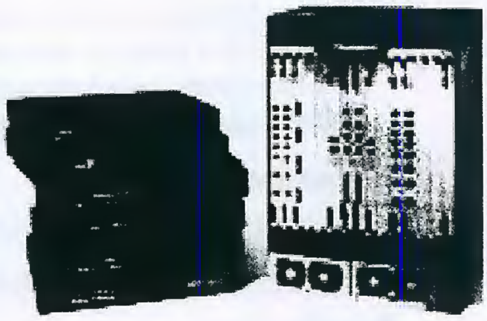
Cisco Content Engine 7300 Series Hardware	
CE-7325-K9	Content Engine 7325 AC Power, ACNSsoftware
CE-7305-K9	Content Engine 7305 AC Power, ACNS software. Also runs as CDM or CR
Cisco Content Engine 500 Series Hardware	
CE-565-K9	Cisco Content Engine 565, AC Power, ACNS software. Also runs as CDM or CR
CE-510-K9	Cisco Content Engine 510 AC Power, ACNSsoftware
Cisco Content Engine Network Module Hardware	
NM-CE-BP-20G-K9=	Content Engine Network Module, basic performance, 20-GB IDE hard disk
NM-CE-BP-40G-K9=	Content Engine Network Module, basic performance, 40-GB IDE hard disk
NM-CE-BP-SCSI-K9(=	Content Engine Network Module, basic performance, SCSI controller (requires external SCSI disk array such as the Cisco SA-6)

[1] This is only a small subset of all parts available via URL listed under "For More Information."

For More Information

See the Cisco Content Engine Web sites: **http://www.cisco.com/go/ce500** and **http://www.cisco.com/go/ce7300**

Cisco CSS 11500 Series Content Services Switches



The Cisco CSS 11500 Series Content Services Switch is suitable for both enterprises and service providers seeking to reduce data center costs, boost e-business application performance, offer enhanced services, ensure online transaction integrity, and provide the best possible online experience for customers, business partners, and internal workers.

The Cisco CSS 11500 is available in three models—the standalone Cisco CSS 11501, the three-slot Cisco CSS 11503 and the six-slot Cisco CSS 11506. Both the CSS 11503 and CSS 11506 systems take advantage of the same high-performance, modular architecture and use the same set of I/O, Secure Sockets Layer (SSL), and session accelerator modules. Also, all three systems operate with the same WebNS software, enabling the Cisco CSS 11501, 11503 and 11506 to offer industry-leading content switching functionality within three compact, hardware platforms.

When to Sell

Sell This Product	When a Customer Needs These Features
CSS 11501	• Standalone, fixed-configuration switching platform with up to 8 Fast Ethernet ports and 1 optional Gigabit Ethernet port • Cost-effective server, cache, and firewall load balancing • Complex Web applications requiring high-level URL and cookie switching
CSS 11503	• Compact, high-performance, modular content switching platform with up to 32 Fast Ethernet ports or up to six Gigabit Ethernet ports • Cost-effective server, cache, and firewall load balancing • Integrated SSL capabilities for secure transactions • Complex Web applications requiring high-level URL and cookie switching
CSS 11506	• Compact, high-performance, modular content switching platform with up to 32 Fast Ethernet ports or up to six Gigabit Ethernet ports • Cost-effective server, cache, and firewall load balancing • Integrated SSL capabilities for secure transactions • Complex Web applications requiring high-level URL and cookie switching

Key Features

- Introduces an intelligent, distributed architecture to meet the real-world scaling requirements of today's e-business infrastructure
- Improves site availability and transaction integrity by introducing Adaptive Session Redundancy (ASR)—a new industry standard in stateful failover
- Delivers the greatest flexibility of any content switch in its class for customizing combinations of ports, performance, and services
- Scales secured transaction performance through support of an integrated, high-capacity Secure Sockets Layer (SSL) module (WebNS 5.20)
- Protects investment by enabling upgrades of performance, ports, and services through modularity

Competitive Products

- Alteon/Nortel: ACEdirector and 700 Series
- F5 Networks: Big/IP and LAN switch Partners
- Foundry Networks: ServerIron
- Radware: Web Server Director (WSD)
- Resonate: Central Dispatch and Global Dispatch

Specifications

Feature	Cisco CSS 11501	Cisco CSS 11503	Cisco CSS 11506
Modular Slots	N/A	3	6
Base Configuration	Switch Control with 8 10/100 Ethernet; 1 GBIC port	Switch Control Module 2 Gigabit Ethernet (GBIC) ports	Switch Control Module 2 Gigabit Ethernet (GBIC) ports
Max GB Ethernet Ports	1	6	12
Max 10/100 Ethernet ports	8	32	80
2-port GB Ethernet I/O Module		Max: 2	Max: 5
16-port GB Ethernet I/O Module		Max: 2	Max: 5
8-port GB Ethernet I/O Module		Max: 2	Max: 5
SSL Module		Max: 2	Max: 5
Session Accelerator modules		Max: 2	Max: 5
Redundancy features	Active-active Layer 5 Adaptive session redundancy Virtual IP Address (VIP) redundancy	Active-active Layer 5 Adaptive Session Redundancy VIP redundancy	Active-active Layer 5 Adaptive Session Redundancy VIP redundancy Active-standby SCM Redundant switch fabric module Redundant power supplies
Height	1/75 in. (1 rack unit)	3.5" (2 rack units)	8.75" (5 rack units)
Bandwidth	Aggregate 6 Gbps	Aggregate 20 Gbps	Aggregate 40 Gbps
Storage	512 MB hard disk or 256 MB Flash disk	512-MB hard disk or 256-MB Flash memory disk	512-MB hard disk or 256-MB Flash memory disk
Power	Integrated AC supply	Integrated AC or DC	Up to 3 AC or 3 DC

Selected Part Numbers and Ordering Information[1]

Cisco CSS 11500 Series Content Services Switches

CSS11506-2AC	Cisco 11506 Content Services Switch including SCM with 2 Gigabit Ethernet ports, hard disk, 2 switch modules, 2 AC power supplies, and a fan (requires SFP GBICs)
CSS11506-2DC	Cisco 11506 Content Services Switch including SCM with 2 Gigabit Ethernet ports, hard disk, 2 switch modules, 2 DC power supplies, and a fan (requires SFP GBICs)
CSS11503-AC	Cisco 11503 Content Services Switch including SCM with 2 Gigabit Ethernet ports, hard disk, and integrated AC power supply, integrated fan, and integrated switch module (requires SFP GBICs)
CSS11503-DC	Cisco 11503 Content Services Switch including SCM with 2 Gigabit Ethernet ports, hard disk, and integrated DC power supply, integrated fan, and integrated switch module (requires SFP GBICs)
CSS5-SCM-2GE	Cisco CSS 11500 System Control Module with 2 Gigabit Ethernet ports and hard disk (requires SFP GBICs)
CSS5-IOM-8FE	Cisco CSS 11500 Fast Ethernet I/O Module: 8-port TX
CSS5-IOM-16FE	Cisco CSS 11500 Fast Ethernet I/O Module: 16-port TX
CSS5-IOM-2GE	Cisco CSS 11500 Gigabit Ethernet I/O Module: 2-port (requires SFP GBICs)
CSS5-SAM	Cisco CSS 11500 Session Accelerator Module
CSS5-SSL	Cisco CSS 11500 SSL Module
CSS11501	Cisco CSS 11501 Content Services Switch-8 Fast Ethernet, hard disk, AC

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the CSS 11500 series Web site: **http://www.cisco.com/go/11500**

Cisco LocalDirector

7647
3

The Cisco Local Director Series offers a high-availability, integrated hardware and software solution that intelligently balances the load of user traffic across multiple TCP/IP application servers. Cisco Local Director tracks network sessions and server load conditions in real time, directing each session to the most appropriate server. All physical servers appear as one virtual server, requiring only a single IP address and a single URL for an entire server farm.

A key component of a content delivery network, Cisco Local Director accelerates content delivery by routing client requests to the best Web server at the Web site of origin. Cisco Local Director supports critical content routing protocols such as Dynamic Feedback Protocol (DFP) and the Boomerang Control Protocol (BCP), which ensure seamless content delivery network integration and reduced deployment costs. Layer 4-7 content load balancing guarantees that the correct client is routed to an optimized content location. The accelerated server load balancing (ASLB) feature works with the Cisco Catalyst 6000 and 6500 Series switches to accelerate scaling of TCP sessions and help to protect against Flash crowds—sudden traffic surges that can overwhelm a web site.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco LocalDirector	• Load balancing across multiple TCP/IP application servers • High availability Internet services such as e-commerce, Web content, and e-mail • High availability Intranet services for employees, customers, and suppliers

Key Features

- HTTP redirect sticky enables client-to-server persistence, regardless of SSL and shopping-cart configurations, to improve site availability
- Hot-standby and stateful failover mechanisms ensures high availability by eliminating all points of failure for the data center
- Transparent support for all common TCP/IP Internet services, including User Datagram Protocol (UDP), accommodates a wide range of applications and communications needs (Web, File Transfer Protocol [FTP], Telnet, Domain Name System [DNS], and Simple Mail Transfer Protocol [SMTP]) without special software configuration
- SSL and cookie sticky ensures completion of complex transactions in proxy server environments
- Client-assigned load balancing provides QoS mechanism by allowing traffic to be directed to servers based on source IP address
- High-performance hardware supports six Fast Ethernet (Cisco Local Director 417) or two Fast Ethernet plus two Gigabit Ethernet (Cisco Local Director 417G) interfaces
- Network Address Translation (NAT) allows unregistered IP addresses on servers without router assistance

- Simple setup in 10 commands offers simple setup for typical configurations, with little disruption to existing network configuration and no changes to network addresses
- Integrated security capability effectively protects server farms from unauthorized access by filtering based on client IP address and service

Competitive Products

- F5 Labs: Big IP
- Foundry Networks: ServerIron Switch
- Nortel Networks/Alteon: Ace Director
- Radware: Web Server Director
- Resonate, Inc.: Central Dispatch

Specifications

Feature	LocalDirector 417	LocalDirector 417G
Supported Interfaces	Six 10/100 BASE-TX	Two 10/100BASE-TX plus two 1000BASE-SX interfaces
Other Interfaces	RJ-45 console interface; DB-15 redundant failover interface	RJ-45 console interface; DB-15 redundant failover interface
RAM	512 MB	512 MB
Flash	16 MB	16 MB
Performance	8000 virtual and real IP addresses 700,000 simultaneous TCP connections 80-Mbps throughput	64,000 virtual and real IP addresses 1,000,000 simultaneous TCP connections 400-Mbps throughput400
Dimensions (HxWXD)	1.72 x 17.5 x 14.13 in	1.72 x 17.5 x 14.13 in

Selected Part Numbers and Ordering Information[1]

Cisco LocalDirector

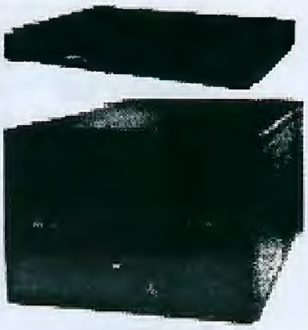
LDIR-417	Cisco Local Director 417
LDIR-417G	Cisco Local Director 417G

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the LocalDirector Web site: **http://www.cisco.com/go/ld**

Cisco Content Distribution Manager 4600 Series



The Cisco Content Distribution Manager (CDM) configures network and device policy settings for edge node Content Engines (CE). Used to accelerate web content and save network bandwidth in a content networking architecture, the CDM can be easily integrated into existing network infrastructures. Deployed in an Enterprise or Service Provider Internet or extranet environment, the Cisco CDM and CEs provide transparent on-demand rich media streaming and static file delivery to standard PCs.

Cisco Enterprise Content Delivery Networks (ECDNs) allow service providers and enterprises to distribute rich media content closer to their target customers overcoming issues such as network bandwidth availability, distance or latency obstacles, origin server scalability, and congestion issues during peak usage periods. The ECDN solution enables content delivery services for web hosting, streaming, e-commerce, e-learning, corporate communications, and mission critical e-business applications.

When to Sell

Sell This Product	When a Customer Needs These Features
CDM 4630	• Low-cost early deployment, or small enterprise network trials, proof of concept, and pilot programs
CDM 4650	• Medium and large enterprise networks, supports up to 1000 Cisco Content Engines
CDM 4670	• Service provider deployment, supports thousands of Cisco Content Engines

Key Features

- Complete CDN solution with Cisco Content Router and Cisco Content Engines
- Central control over delivery of high-bandwidth content, live and video-on-demand over any IP network
- Easy-to-use management capabilities through a Web-based GUI; services include previewing and scheduling replication of media to edge devices, bandwidth and content management
- Automatically generates thumbnail reference images and sample Web pages for integration with corporate extranet, intranet, and Internet sites
- One URL per media file provides seamless integration into any Web site
- Integrates with standards for Web multimedia presentation, including HTML/DHTML, eXtensible Markup Language (XML) and SMIL
- Secure and fault-tolerant file transfer using Secure Socket Layer (SSL) encryption for secure media transfers
- Channel configuration for media distribution to any number of discrete audiences using "distribution lists"
- Host content for a variety of customers within a single CDN
- Ability to create multiple virtual CDNs addressing targeted media distribution
- Content registration in cache logs for billing capabilities

Competitive Products

- Cacheflow: Client and Server Accelerators
- Inktomi: Traffic Server
- Network Appliance: ContentDirector

Specifications

Feature	Content Distribution Manager 4630	Content Distribution Manager 4650	Content Distribution Manager 4670
Sampling of Rich Media File Formats	MPEG RealVideo Windows Media QuickTime HTML, GIF, JPEG Adobe Acrobat Macromedia Shockwave CAD/CAM MRI	Same as CDM 4630	N/A—file formats handled by the CEs
Supported Interfaces	Autosensing 10/100BASE-T	Autosensing 10/100BASE-T	Autosensing 10/100BASE-T
Recommended Network Size	Less than 100 CEs	Less than 1000 CEs	Less than 10,000 CEs
Processor Speed	600-MHz PIII	2x866 Xeon	2x866 Xeon
RAM	512 MB	1 GB	1 GB
Internal Storage	One 30 GB, 10K RPM, Ultra2 SCSI disk drive	140 GB RAID 5	36 GB[1]
Rack Units	1	7	7
Dimensions (HxWXD)	1.72 x 17.5 x 14.1 in.	12.25 x 17.5 x 28 in.	12.25 x 17.5 x 28 in.

[1] Minimum storage required for DM service provider configurations

Selected Part Number and Ordering Information[1]

Cisco Content Distribution Manager 4600 Series Hardware	
CDM-4630	Cisco Content Distribution Manager 4630
CDM-4650	Cisco Content Distribution Manager 4650
CDM-4670	Cisco Content Distribution Manager 4670

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Content Distribution and Management Web site:
http://www.cisco.com/go/cdm

Cisco Content Router 4430

The Cisco Content Router 4430 (CR 4430) is a compact, high-performance solution for enabling premium Web services over public or private networks. Featuring either Cisco Enterprise Content-Delivery Network (ECDN) or Content Router 1.1 Software, customers can transparently route user Web browsers to the optimal content engine for file delivery.

With its patented routing technology, the Cisco CR 4430 provides redundancy, scalability, and performance enhancements for network Web sites in either an enterprise or public service provider network. Using Hypertext Transfer Protocol (HTTP)-based re-direction, the Cisco CR 4430 can redirect users over the public network or behind the security of a corporate firewall, making it a vital component of the Cisco end-to-end Content Networking Solution.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Content Router 4430	• When a customer needs to support a Cisco Enterprise Content Delivery Network with HTTP redirection • Supports resiliency for ECDNs when used with a Cisco CSS 11500 content services switch • Up to five Cisco CR 4430s can be deployed in an ECDN network to provide greater network availability and performance

Key Features

- Uses HTTP to redirect a client to the best site on the Internet based on network delay
- Transparent redirection to the end user and works with any IP application
- Easy configuration through a Cisco IOS-style command-line interface
- Redundant configurations, multiple CRs can be deployed at the origin site to provide fail-over and load scaling

Specifications

Feature	Cisco Content Router CR4430
Network Interface Card	10/100BASE-TX
Processor	600- MHz PIII
RAM	1 GB
Internal Storage	18 GB
Rack Units	1
Dimensions (HxWXD)	1.72 x 17.50 x 14.13 in.
Weight	12.5 lbs.

Selected Part Number and Ordering Information

Cisco Content Routers	
CR-4430	Content router that utilizes HTTP redirection for use with the ECDN product

For More Information

See the Cisco Content Router Web site: **http://www.cisco.com/go/cr**

Cisco Content Switching Module

The Cisco Content Switching Module (CSM) is a Catalyst 6500 line card that balances client traffic to farms of servers, firewalls, SSL devices, or VPN termination devices. The CSM provides a high-performance, cost-effective load balancing solution for enterprise and Internet Service Provider (ISP) networks. The CSM meets the demands of high-speed Content Delivery Networks, tracking network sessions and server load conditions in real time and directing each session to the most appropriate server. Fault tolerant CSM configurations maintain full state information and provide true hitless failover required for mission-critical functions.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Content Switching Module	• An integrated load balancing solution featuring Cisco's Catalyst 6500 • Load balancing for the highest traffic sights • Support for up to 1,000,000 concurrent TCP connections

Key Features

- Market-leading performance—Establishes up to 200,000 Layer 4 connections per second and provides high-speed content switching, while maintaining 1 million concurrent connections
- Outstanding price/performance value for large data centers and ISPs—Features a low connection cost and occupies a small footprint. The CSM slides into a slot in a new or existing Catalyst 6500 and enables all ports in the Catalyst 6500 for layer 4 through layer 7 content switching. Multiple CSMs can be installed in the same Catalyst 6500
- Uses the same Cisco IOS Command Line Interface (CLI) that is used to configure the Catalyst 6500 Switch

Competitive Products

- Alteon/Nortel: ACEdirector and 700 Series
- Radware: Web Server Director (WSD)
- F5 Networks: Big/IP and LAN switch Partners
- Foundry Networks: ServerIron
- Resonate: Central Dispatch and Global Dispatch

Specifications

Feature	Cisco Content Switching Module (CSM)
Configuration Limits	256 total VLANs (client and server); 4000 virtual servers; 4000 server farms; 16,000 real servers; 4000 probes; 16,000 access control list (ACL0 items
Connections	1,000,000 concurrent TCP connections 200,000 connection setups per second-Layer 4
Throughput	4 Gigabits-per-second total combined (client-to-server and server-to-client) throughput
Catalyst Switch Platform Requirements	Cisco IOS Software only—Catalyst Operating System is not supported Functions as a bus enabled line card—not fabric enabled Multilayer switch feature card-MSFC or MSFC2

Selected Part Numbers and Ordering Information[1]

Cisco Content Switching Module

WS-X6066-SLB-APC	Catalyst 6500 Content Switching Module

For More Information

See the Catalyst 6500 Series Web site at: **http://www.cisco.com/go/cat6500**

Cisco SSL Module for Catalyst 6500

The SSL Services Module is an integrated service module for the Cisco Catalyst® 6500 Series that offloads the processor-intensive tasks related to securing traffic with Secure Sockets Layer (SSL) and increases the number of secure connections supported by a Web site.

When to Sell

Sell This Product	When a Customer Needs These Features
SSL Module for Catalyst 6500	• An integrated SSL encryption/decryption solution featuring Cisco's Catalyst 6500 • Scalable SSL processing: 2,500 connection setups/second per module-10,000 per Chassis fully-populated with SSL modules

Key Features

- Server SSL offload—performs all SSL-related tasks, allowing servers to handle high-speed clear text traffic
- Scalable performance—provides a simple means of addressing increased performance requirements by installing additional SSL modules in a Catalyst 6500 switch
- Stickyness—maintains persistence even when clients request new session IDs, in Integrated Mode with Content Switching Module (CSM)
- Certificate optimization—provides cost savings by requiring only a single certificate copy vs. a copy for each server subject to customer and certificate authority agreement

Competitive Products

• F5 Networks eCommerce 540	• Nortel/Alteon iSD 410 SSL Accelerator

Specifications

Feature	Cisco SSL Module for Catalyst 6500
System Capacity and Performance	2500 connection setups/sec per module-10K per chassis; 60K concurrent client connections-240K per chassis; 300 Mbps bulk rate encryption-1.2 Gbps per chassis; 256 key pairs; 256 key certificates; Up to 2K key sizes;256 proxy servers
Scalability	Up to four SSL modules in the same Catalyst 6500
Integration with Server Load Balancing	Tightly integrated in the Cisco Catalyst 6500 Switch with the CSM

Selected Part Numbers and Ordering Information[1]

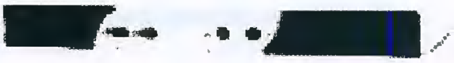
Cisco SSL Module for Catalyst 6500

WS-SVC-SSL-1-K9=	Cisco SSL Module for Catalyst 6500

For More Information

See the Catalyst 6500 Series Web site at: **http://www.cisco.com/go/cat6500**

Cisco 11000 Series Secure Content Accelerator (SCA 11000)



The Cisco 11000 Series Secure Content Accelerator (SCA 11000) is an appliance-based solution that increases the number of secure connections supported by a Web site by offloading the processor-intensive tasks related to securing traffic with SSL. Available in two versions, the SCA 11000 simplifies security management and allows Web servers to process more requests for content and handle more e-transactions.

7641
3

Key Features

- Offloads all encryption, decryption, and secure process for a Web site, freeing Web servers to perform essential Web tasks and eliminating the need for SSL server software
- Boosts e-commerce site performance up to 50 times through dedicated SSL processing hardware—supports 200 or 800 new SSL connections per second
- Centralizes and manages the widest range of digital certificates to ensure complete independence from the Web server
- Provides linear scalability and fault tolerance—interoperates with the Cisco 11500 series Content Services Switches (CSS 11500) for intelligent load balancing of SSL traffic
- Works with any Web server platform to provide SSL support for any Web site
- Installs quickly and easily with very low maintenance—no special software required on Web servers or Cisco 11500 series switches

Specifications

Cisco SCA 11000	SCA2	SCA
Number of Ports	Two 10/100BaseTX Ports	Two 10/100Base TX Ports
Port Description	Network Ports: Two 10/100Base TX; Console Port: DB9 Serial Port; Failover Port: DB9 Serial Port	Network Ports: Two 10/100Base TX; Console Port: DB9 Serial Port; Failover Port: DB9 Serial Port
Data Transfer Rates	Ethernet: 10 Mbps (half duplex), 20 Mbps (full duplex)Fast Ethernet: 100 Mbps (half duplex), 200 Mbps (full duplex)	Ethernet: 10 Mbps (half duplex), 20 Mbps (full duplex) Fast Ethernet: 100 Mbps (half duplex), 200 Mbps (full duplex)
Configuration Software OS Support	Windows NT 4.0; Red Hat Linux 5.0, 6.0, 6.1, 6.2	Windows NT 4.0; Red Hat Linux 5.0, 6.0, 6.1, 6.2
Memory	64 MB RAM; 16 MB Flash ROM	64 MB RAM; 16 MB Flash ROM
Dimensions	8.875 x 1.75 x 19 in.	8.875 x 1.75 x 19 in.
Connection Rates	800	200
Concurrent Sessions	5,000	30,000

Selected Part Numbers and Ordering Information

Cisco SCA 11000

CSS-SCA-2FE-K9	CSS Secure Content Accelerator
CSS-SCA2-2FE-K9	CSS Secure Content Accelerator version 2

For More Information

See the Cisco SCA 11000 Web site: **http://www.cisco.com/go/sca11000**

Cisco CTE-1400 Series Content Transformation Engine

The Cisco CTE 1400 Series Content Transformation Engine provides customers with a high-performance, appliance-based solution that delivers real business applications and Internet content to a variety of devices including Wireless Application Protocol (WAP) phones, personal digital assistants (PDAs), Blackberry pagers, Cisco IP Phones and other non PC devices. Examples of applications that can be transformed include e-mail, CRM/SFA applications, intranets, maps, directions, and corporate directories as well as many vertical applications in healthcare, retail, finance, hospitality and education. The Content Transformation Engine (CTE) is a 1 Rack Unit appliance optimized to perform the task of converting HTML and XML applications to a format appropriate for devices with unique display requirements. In addition, the solution recognizes specific Web-enabled devices such as IP Phones, PDAs and mobile phones, and customizes the delivery of information to give users the right form of data, to suit their devices characteristics, capability as well as the usage model.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco CTE-1400 Series Content Transformation Engine	• Quickly and easily transform applications to extend them to a variety of new devices. • Low total cost of ownership (TCO) • Immediate results for a rapid return on investment • Self-contained appliance optimized for transformation

Key Features

- Self-contained appliance for content transformation; includes DesignStudio for defining transformation rules
- Seamlessly transforms content as it moves from server to the target device, leaving the server and underlying data unchanged; Reformats data into all major Markup Languages
- Supports Cisco's AVVID architecture, including transformation for Cisco IP telephony
- Low total cost of ownership

Specifications

Feature	Cisco CTE-1400 Series Content Transformation Engine
Rack Units	1
Dimensions (HxWxD)	1.70 x 16.7 x 22in.
Weight	23 lbs

Selected Part Numbers and Ordering Information[1]

Cisco CTE 1400 Series Content Transformation Engine

CTE-1450-K9	Content Transformation Engine Hardware
CTE-WAP=	WAP module for CTE 1400 Series
CTE-PALM=	Palm module for CTE 1400 Series
CTE-RIM=	RIM Blackberry module for CTE 1400 Series
CTE-HTML=	HTML module for CTE 1400 Series

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the CTE-1400 Series Web site at **http://www.cisco.com/go/cte**

Cisco DistributedDirector[1]

DistributedDirector provides dynamic, transparent, and scalable Internet traffic load distribution between multiple geographically-dispersed servers. DistributedDirector is a global Internet service-scaling solution that utilizes Cisco IOS software and leverages routing table information, delay characteristics, and other information to make “network intelligent” load distribution and site selection decisions.

DistributedDirector transparently redirects end-user service requests to the closest responsive server, which increases access performance and reduces transmission costs. Users need only a single subdomain name or URL-embedded hostname for accessing a distributed set of servers, thus providing the appearance of a single virtual server.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Distributed Director	• Load distribution across geographically/topologically dispersed TCP/IP servers • High availability for dispersed mission-critical applications • Data center redundancy and failover

Key Features

- Transparent distribution of all IP Services (TCP and UDP), including HTTP, FTP, Telnet, and Gopher; provides global scalability for all IP-based network services
- Improves access performance by redirecting to the topologically closest server
- Calculates client-to-server round-trip times in real time; redirects clients to server with lowest client-to-server link latency, maximizing end-to-end performance
- Redirects clients only to responsive servers, resulting in maximized availability
- Cisco IOS Software & standard command line interface for device configuration
- Transparently add and remove distributed servers, simplifying maintenance
- Supports multiple domains; cost-effective IP service scalability solution

Competitive Products

- Alteon Networks: ACEdirector and Web Switches with WebOS GLSB
- F5 Labs: 3DNS
- Foundry Networks: ServerIron Switch with Internet IronWare
- Resonate, Inc.: Global Dispatch
- RND Networks, Inc.: Web Server Director - Network Proximity (WSD-NP)

For More Information

See the DistributedDirector Web site at **http://www.cisco.com/go/dd**

[1] DistributedDirector is available in Cisco IOS software for 2600/2600XM, 3600, and 7200 series routers, starting on release 12.2(4)T Enterprise Plus feature sets; Dedicated routers may be recommended for DistributedDirector to meet performance targets of both routing and load balancing; If no dedicated hardware platform is available for running DistributedDirector, it is recommended customers use the Configurable DD Cache feature (available in 12.2(8)T) to limit the memory DistributedDirector may consume for DNS caching; To take advantage of enhanced caching capabilities, routers should be configured with additional DRAM (128MB or more)

Cisco GSS 4480 Global Site Selector

The Cisco GSS 4480 is a networking product that globally load balances distributed data centers. The Cisco GSS 4480 acts as the cornerstone of multisite disaster recovery plans in deployments of Cisco's market-leading content switches. Customers deploying new Cisco content switches such as the Cisco CSS 11500 Content Services Switch and the Content Switching Module (CSM) for the Cisco Catalyst ® 6500 Series switches or have already deployed legacy switches such as the Cisco CSS 11000 and Cisco Local Directors can benefit from the new levels of traffic management and centralized command and control provided by the Cisco GSS 4480.

Key Features

- Provides resilient architecture critical for disaster recovery and multisite Web applications deployments
- Offers flexible heterogeneous support for all Cisco SLBs and DNS-capable networking products
- Provides centralized command and control of DNS resolution process for direct and precise control of global load-balancing process
- Offers site persistence for e-commerce applications
- Offers a unique DNS race feature-The Cisco GSS 4480 can in real time direct content consumers to the closest data center
- Supports a Web-based graphical user interface (GUI) and DNS wizard to simplify the DNS command and control

Competitive Products

• F5 Networks eCommerce 540	• Nortel/Alteon iSD 410 SSL Accelerator

Specifications

Feature	Cisco GSS 4480
Number of Ports	Two 10/100Base TX Ports
Port Description	Network Ports: Two 10/100Base TX; Console Port
DNS requests per second	4000, depending on configuration (~ 345 million DNS requests per day per Cisco GSS 4480; an entire system is capable of 2.7 billion DNSrequests per day)
Configuration Software OS Support	Windows NT 4.0; Red Hat Linux 5.0, 6.0, 6.1, 6.2
Network management	Console port-CLI Access to system via Telnet; Secure copy (SCP) or FTP; GUI-Secure HTTP (HTTPS) for Internet Explorer and Netscape Navigator
Storage	One 36-GB hard drive
Physical	One-rack unit size chassis; Network management serial port1 GB of RAM600-MHz PIII CPU
Dimensions	1.72 x 17.5 x 14.13 in. (43.7 x 444.5 x 358.9 cm)

Selected Part Numbers and Ordering Information[1]

Cisco GSS 4480

Cisco GSS 4480-K9	Global site selector
SF-GSS-V1.0-K9	SF-GSS-V1.0-K9Global site selector software

For More Information

See the Cisco GSS 4480 Web site: **http://www.cisco.com/go/gss**

CHAPTER 7

Broadband and Dial Access Products

Broadband and Dial Access Products at a Glance

Remote Dial Access—Data and Voice (VoIP)

Product[1]	Features	Page
Cisco AS5350 Series Universal Gateways	• High performance, 1RU, universal gateway • Universal Port technology for multiple data, voice, and fax services on any port at any time • 2,4, & 8 CT1/7 CE1/PRI configurations for 48 to 240 channels • Supports broad range of async/ISDN/VoIP/wireless protocols • Two 10/100 Ethernet ports, two 8 Mbps serial backhaul ports • Two 8 Mbps serial backhaul ports • Cisco SS7 signaling gateway interoperability • Flexible, redundant backhaul methods	7-3
Cisco AS5400 Series Universal Gateways	• High performance, 2RU, universal gateway • Universal Port technology for multiple data, voice, and fax services on any port at any time • Two models: Cisco AS5400HPX and Cisco AS5400 • 8 to 16 CT1/CE1/PRI or 1 T3 configuration for 192 to 648 channels • Low power and high availability design • Supports a broad range of async/ISDN/VoIP/fax/wireless protocols • Cisco SS7 signaling gateway interoperability • Flexible, redundant backhaul methods	7-6
Cisco AS5850 Universal Gateway	The highest density universal gateway in the marketplace • Supporting up to 5 x CT3s, 96 T1s or 86 E1s of multiple data, voice, and fax services on any port at any time • Constant density regardless of codec type, ECAN or VAD settings • Extensive high availability features • TDM grooming capability	7-9
Remote Dial Access Network Management	Suite of network management products for configuration, troubleshooting, and maintenance of Cisco dial access and VoIP solutions	7-11
SS7 Signaling & Softswitch Products	• Cisco PGW 2200 Softswitch—Call Agent providing signaling and call control functionality for PSTN Gateway and transit applications in international markets • Cisco BTS 10200 Softswitch—MGCP-based softswitch for large-scale Voice over IP and ATM applications	7-12

1. For Cisco 2509 and 2511 Access Servers, see page 1-14.

Broadband Cable

Product	Features	Page
Headend and Distribution Hub Equipment		
Cisco uBR7100 Series Universal Broadband Router	Entry-level, fixed-configuration CMTS and integrated router for lower-density residential and MxU customers serviced by Tier 2/Tier 3 cable operators or ISPs. • Choice of four DOCSIS- and EuroDOCSIS-qualified, fixed-configuration models that include: Cisco uBR7111, Cisco uBR7111E, Cisco uBR7114, and Cisco uBR7114E • Integrated upconverter/modulator on the cable interface • Embedded dual 10/100 BaseT Ethernet network interface • Additional network interface with a variety of LAN and WAN options • Supports up to 1,000[1] data customers	7-13
Cisco uBR7246VXR Universal Broadband Router	• Modular, standards-based communications-grade CMTS and integrated router for high-growth broadband cable deploymentsSupports up to 8,000 subscribers and offers a large variety of LAN and WAN interface options and processors	7-15

7635
E

Product	Features	Page
Cisco uBR10012 Universal Broadband Router	Highest-capacity communications-grade CMTS and integrated router on the market today that delivers the services, performance, scale, and carrier-class reliability large cable operators and ISPs demand • High-performance aggregation platform that uses Parallel Express Forwarding technology • Eight cable line cards that include support for Cisco Universal Broadband Router (uBR) line cards and the Cisco 5X20 Broadband Processing Engine (BPE) • Four network interfaces that include support for 1 Gbps over Gigabit Ethernet, 622 Mbps over OC-12 Packet over SONET, and OC-48-Dynamic Packet Transport (DPT) Interface Module Set • Cisco uBR10012 supports up to 80,0001 subscribers	7-16
Cisco RF Switch	• Exceeds PacketCable Availability Requirements • Enables a fully redundant CMTS with no single point of failure; works with the Cisco uBR7246VXR and uBR10012 • Maximizes density with more than 250 MCX-type connector	7-17
Customer Premise Equipment (CPE)		
Cisco uBR900 Series Cable Access Router	Integrated DOCSIS-based cable modem and router with hardware accelerated IPSec VPN tunneling support that includes: • Cisco uBR925 with 4 Ethernet, 1 CATV, 1 USB and 2 FXS ports that support telecommuter and small office DOCSIS-based data, VoIP, and VPN services • Cisco uBR905 with 4 Ethernet and 1 CATV port that supports DOCSIS-based data and VPN services	7-19

1. Numbers are for reference only. Actual numbers for specific systems will vary depending on network/service loading, traffic, and other parameters.

DSL (Digital Subscriber Line) Access

Product	Features	Page
DSL Access CPE[1]	Wide variety of Cisco router-based DSL CPE solutions for business-class to small office applications	7-21
Broadband Services Aggregation	• Cisco 6400 Series Router—ATM switching core, with up to 48,000 subscriber sessions per chassis • Cisco 7200 Series Router—Up to 16000 broadband sessions on a 3 RU platform, including aggregation of PPP, PPPoE, and PPPoA • Cisco 7301 Series Router—1 RU Broadband Aggregation Router that is capable of delivering up to 16000 sessions per chassis • Cisco 7400 Series Router—1 RU broadband optimized appliance that delivers up to 8,000 sessions per chassis • Cisco 10000 Series Router—A carrier-class router that supports up to 32,000 broadband sessions with 99.999 percent system uptime	7-21

1. For ADSL, ISDN, and IDSL small office/home office (SOHO) customer premise equipment (CPE), see Chapter 1: Routers

ATM Multiservice WAN Switching

Product	Features	Page
Cisco BPX 8600 Series Switches	• Large-scale Advanced ATM switch for service provider and large enterprise applications • Narrowband and broadband services in a single, highly reliable platform using a multishelf architecture with intelligent call processing for Frame Relay and ATM switched virtual circuits (SVCs) • 20 Gbps of high-throughput switching for multiple traffic types data, voice, and video	7-23
Cisco MGX 8850 Series Advanced ATM Multiservice Switches	• Multiservice switch, scales from DS0 to OC-48c/STM-16 speeds • Serves as a stand-alone device for narrowband services, an integrated edge concentrator or a broadband edge switch when equipped with 45 Gbps switch card and broadband ATM modules	7-24
Cisco MGX 8830 Series Multiservice Switches	• Multiservice switch scales from from DS0 to OC-3c/STM-1 speeds • A standalone switch with narrowband interfaces and broadband trunking to remote sites with low density and high service mix requirements with 1.2 Gbps switch fabric	7-25
Cisco IGX 8400 Series Multiservice WAN Switches	• ATM-based WAN switching, connects to public services for reduced leased-line costs • Available with 8, 16, or 32 slots	7-25
Cisco MGX 8200 Series Multiservice Gateways	• Edge concentrators family provide a cost-effective narrowband multiservice solution for low to mid-band ATM and Frame Relay aggregation with QoS management features	7-25

Long Reach Ethernet

Product	Features	Page
Cisco Catalyst 2950 LRE XL Switches	Fixed configuration Ethernet switches for delivering converged voice, video, and data services over existing category 1/2/3 wiring for the MxU and enterprise markets. • 12- or 24-port 1RU switchesystems with four 10/100 ports, deliver Ethernet traffic (up to 15 Mbps) over standard copper cabling (up to 5000 feet); ideal for MxU broadband Internet access • Co-exists with POTS and ISDN traffic on the same line and compatible with ADSL • Advanced quality of service for supporting converged voice, video, and data services	7-26
Cisco LRE CPE Devices	• Cisco 575 LRE CPE—Compact, includes one RJ-45 Ethernet connection and two RJ-11 connectors (for telephone) • Cisco 585 LRE CPE—Compact, includes four RJ-45 switched Ethernet connections and two RJ-11 connectors (for telephone). Supports 802.1p QoS	7-27
Cisco LRE POTS Splitter	• Cisco LRE 48 POTS Splitter—48 ports in 1RU. Ensures that POTS service is separate, and never compromised by LRE switch reconfiguration or downtime	7-27
Cisco Broadband Building Service Manager	• Server system enables automated online activation, integrated billing, tiered service levels • Ideal for any form of broadband access technology, including Ethernet, LRE, Cable access, DSL, Wireless, or Fiber	7-28

Memory Information for Access Routers

Router	Memory Type	Slots	Default Memory	Max Memory	Default Config. (Notes)
Cisco AS5350 Universal Gateway	System Flash SDRAM Shared Boot Flash	N/A	32 MB 128 MB 64 MB 8 MB	64 MB 512 MB 128 MB 16 MB	
Cisco AS5400HPX Universal Gateway	Main SDRAM Shared Boot Flash (3V) System Flash (3V)	2 1 1 2	256 MB 64 MB 8 MB 32 MB	512 MB 128 MB 16 MB 64 MB	Cisco AS5400HPX and Cisco AS5400 use different Boot and System Flash — NOT interchangeable
Cisco AS5400 Universal Gateway	Main SDRAM Shared Boot Flash (5V) System Flash (5V)	2 1 1 2	256 MB 64 MB 8 MB 32 MB	512 MB 128 MB 16 MB 64 MB	Cisco AS5400HPX and Cisco AS5400 use different Boot and System Flash — NOT interchangeable
Cisco AS5850 Universal Gateway	RSC SDRAM Feature Cards SDRAMS		512 MB 128 MB	512 MB 128 MB	Ships with all required memory
Cisco CVA120 Series	Config NVRAM DRAM Flash		128 kB 16 MB 8 MB		

Cisco AS5350 Universal Gateway

The Cisco AS5350 Universal Gateway is the only one-rack-unit gateway supporting two-, four-, or eight-port T1/seven-port E1 configurations that provides universal port data, voice, and fax services on any port at any time. The Cisco AS5350 Universal Gateway offers high performance and high reliability in a compact, modular design. This cost-effective platform is ideally suited for Internet service providers (ISPs) and enterprise companies that require innovative universal services.

The Cisco AS5350 Universal Gateway eliminates the need for switches and routers to create a point-of-presence (POP) or "POP-in-a-box" solution. The Cisco AS5350 Universal Gateway has three primary universal gateway configurations: two Channelized T1(CT1)/Channelized E1(CE1)s, four CT1/CE1s, and eight CT1/seven CE1s . It also includes integrated signaling link termination (SLT) functionality for direct connection to a SS7/C7 signaling gateway.

The Cisco AS5350 Universal Gateway comes two high-speed serial ports are provided to support Frame Relay, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC) backhaul. All backhaul interfaces support Hot Standby Router Protocol (HSRP), and all cards and the fan tray are hot-swappable for carrier-class resiliency. The Cisco AS5350 Universal Gateway is the only access server in this form factor that offers universal port capability with these high-availability features.

4633 ω

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco AS5350	• 2 to 8 channelized CT1/7 CE1/PRI compact and modular universal • High-performance modem, ISDN, and voice call termination • Universal port services (data, voice, fax)

Key Features

- 1 RU modular high-performance 2 to 8 channelized CT1/7 CE1/PRI system
- Universal Gateway—which supports multiple data, voice, and fax services on any port at any time
- Ideal for Tier 2/3 ISPs and enterprises requiring innovative universal services
- Feature cards: 2, 4, or 8 CT1/7 E1/PRI feature cards (ISDN calls terminated on the card); 60 or 108 channel Universal Port feature card
- Two 10/100BaseT autosensing Ethernet LAN ports
- Two 8 MB serial WAN ports for Frame Relay, HDLC, or PPP WAN backhaul
- Carrier Class Resiliency: All feature cards and fan tray are hot swappable, modem and voice DSP are pooled and can be configured as spares, AC internal power supply with dual fans, Redundant LAN/WAN backhaul ports, Thermal management and environmental monitoring, ETSI/NEBS Level 3 compliant
- Cisco SS7 signaling gateway interoperability

Competitive Products

- Lucent/Ascend: Max TNT
- 3Com/CommWorks: Total Control 1000
- Alcatel: 7505 Series
- Nuera: BTX Series
- Siemans: HiPath Series

Specifications

Feature	Cisco AS5350
Processor	250 MHz RISC processor
Memory	SDRAM: 128 MB (default), 512 MB (maximum) Shared Input/output (I/O): 64 MB (default), 128 MB (maximum) Boot Flash: 8 MB (default), 16 MB (maximum) System Flash: 32 MB (default), 64 MB (maximum) Layer 3 Cache: 2 MB
Feature Card Slots	Three slots
Egress Ports	Two 10/100-MB Ethernet ports Two 8-Mbps serial ports T1/E1 DS1 trunk feature cards
LAN Protocols	IP, IPX, AppleTalk, DECNet, ARA, NetBEUI, bridging, HSRP, 802.1Q
WAN Protocols	Frame Relay, PPP, HDLC (leased line)
Routing Protocols	RIP, RIPv2, OSPF, IGRP, EIGRP, BGPv4, IS-IS, AT-EIGRP, IPX-EIGRP, Next Hop Resolution Protocol (NHRP), AppleTalk Update-Based Routing Protocol (AURP)
QoS Protocols	IP Precedence, Resource Reservation Protocol (RSVP), Weighted Fair Queuing (WFQ), Weighted Random Early Detection (WRED), Multichassis Multilink PPP (MMP) fragmentation and interleaving, 802.1P
Access Protocols	PPP, Serial Line Internet Protocol (SLIP), TCP Clear, IPXCP, ATCP, ARA, NBFCP, NetBIOS over TCP/IP, NetBEUI over PPP, protocol translation (PPP, SLIP, ARA, X.25, TCP, local-area transport [LAT], Telnet), and Xremote
Bandwidth Optimization	Multilink PPP (MP), MLP, TCP/IP header compression, Bandwidth Allocation Control Protocol (BACP), bandwidth on demand, nonfacility-associated signaling (NFAS), traffic shaping
Voice Compression	G.711, G.723.1, (5.3K and 6.3K), G.726, G.729ab, G.Clear, GSM-FR
DSP Voice Features	Echo cancellation, programmable up to 128 ms Transparent transcoding between A-law and mu-law encoding Voice activity detection, silence suppression, comfort noise generation Fixed and adaptive jitter buffering Call progress tone detection and generation - Dial tone, busy, ring-back, congestion, and re-order tones with local country variants DTMF, Multifrequency (MF) Continuity Testing (COT)

Feature	Cisco AS5350
Voice and Fax Signaling Protocols	H.323v2, H.323/v3, H.323v4, SIP, MGCP 1.0, TGCP 1.0, Voice Extensible Markup Language (VoiceXML), Real-Time Streaming Protocol (RTSP), Extended Simple Mail Transfer Protocol (ESMTP) T.38 real-time fax relay T.37 fax store and forward Fax detection Fax and modem passthrough Open Settlements Protocol (OSP) Media Recording Control Protocol (MRCP) Text to Speech (TTS) Servers Automatic Speech Recognition (ASR) Servers
SS7	Integrated SLT functionality
Network Security	RADIUS or TACACS+ PAP or CHAP authentication Local user/password database DNIS, CLID, call-type preauthentication Inbound/outbound traffic filtering (including IP, IPX, AppleTalk, bridged traffic) Network Address Translation (NAT) Dynamic access lists SNMPv2, SNMPv3
Virtual Private Networking	IP Security (IPSec) Policy enforcement (RADIUS or TACACS+) L2TP, Layer 2 Forwarding (L2F), and generic routing encapsulation (GRE) tunnels Firewall security and intrusion detection QoS features (committed access rate [CAR], Random Early Detection [RED], IP Precedence, policy-based routing)
Channelized T1	Robbed-bit signaling; Loop Start, Immediate Start, and Wink Start Protocols
Channelized El	CAS, PRI, E1 R1, E1 R2, leased line, Frame Relay, G.703, G.704
ISDN Protocols Supported	Sync mode PPP, V.120, V.110 at rates up to 38400 bps Network- and User-side ISDN NFAS with backup D-channel QSIG, Feature Group B, Feature Group D DoVBS
Modem Protocols Supported	V.90 or V.92 standard supporting rates of 56000 to 28000 in 1333 bps increments V.92 Modem on Hold V.44 Compression Fax out (transmission) Group 3, standards EIA 2388 Class 2 and EIA 592 Class 2.0, at modulations V.33, V.17, V.29, V.27ter, and V.21 K56Flex at 56000 to 32000 in 2000 -bps increments ITU-T V.34 Annex 12 at 33600 and 31200 bps and many others
Wireless Protocols Supported	V.110, V.120
Full Cisco IOS Support	IP Plus and Enterprise Plus feature sets
Console and Auxiliary Ports	Asynchronous serial (RJ-45)
Chassis	Dimensions (H x W x D): 1.75 x 17.5 x 20.5 in. Weight (fully loaded): 22 lbs. (10 kg)

Selected Part Numbers and Ordering Information[1]

Cisco AS5350 Universal (Data) System Bundles

AS535-2T1-48-AC	AC AS5350; 2T1, 60 ports, IP+ IOS, 48 Data Lic
AS535-4T1-96-AC	AC AS5350; 4T1, 108 ports, IP+ IOS, 96 Data Lic
AS535-8T1-192-AC	AC AS5350; 8T1, 216 ports, IP+ IOS, 192 Data Lic
AS535-2E1-60-AC	AC AS5350; 2E1, 60 ports, IP+ IOS, 60 Data Lic
AS535-4E1-120-AC	AC AS5350; 4E1, 120 ports, IP+ IOS, 120 Data Lic
AS535-8E1-210-AC	AC AS5350; 8E1,216 ports,240 ISDN ports, IP+ IOS,210 Data Lic

Cisco AS5350 Universal (Voice) System Bundles

AS535-2T1-48-AC-V	AC AS5350 Voice; 2T1, 60 ports, IP+ IOS, 48 Voice Lic
AS535-4T1-96-AC-V	AC AS5350 Voice; 4T1, 108 ports, IP+ IOS, 96 Voice Lic
AS535-8T1-192-AC-V	AC AS5350 Voice; 8T1, 216 ports, IP+ IOS, 192 Voice Lic
AS535-2E1-60-AC-V	AC AS5350 Voice; 2E1, 60 ports, IP+ IOS, 60 Voice Lic
AS535-4E1-120-AC-V	AC AS5350 Voice; 4E1, 120 ports, IP+ IOS, 120 Voice Lic
AS535-8E1-210-AC-V	AC AS5350 Voice; 8E1, 216 ports, IP+ IOS, 210 Voice Lic

Cisco AS5350 Spare Chassis

AS5350-AC=	AC 5350 Chassis with Motherboard, IP Plus IOS, default memory
AS5350-DC=	DC 5350 Chassis with Motherboard, IP Plus IOS, default memory

Cisco AS5350 Software	
S535AK8-12202XA	Cisco AS5350 Series IOS ENTERPRISE PLUS IPSEC 56
S535AP-12202XA	Cisco AS5350 Series IOS ENTERPRISE PLUS
S535CK8-12202XA	Cisco AS5350 Series IOS IP PLUS IPSEC 56
S535CP-12202XA	Cisco AS5350 Series IOS IP PLUS
Cisco AS5350 Memory Options & Spares	
MEM-UP1-AS535	16M Bootflash,64M System Flash,256M Main,128M Shared I/O Memory
MEM-16BF-AS535	AS5350 16MB Boot Flash upgrade
MEM-64F-AS535	AS5350 64MB System Flash upgrade
MEM-256M-AS535	AS5350 256MB Main SDRAM upgrade
MEM-128S-AS535	AS5350 128MB Shared I/O upgrade
Cisco AS5350 Spare DFC Boards	
AS535-DFC-2CT1=	AS5350 Dual T1/PRI DFC card
AS535-DFC-2CE1=	AS5350 Dual CE1/PRI DFC card
AS535-DFC-4CT1=	AS5350 Quad T1/PRI DFC card
AS535-DFC-4CE1=	AS5350 Quad E1/PRI DFC card
AS535-DFC-8CT1=	AS5350 Octal T1/PRI DFC card
AS535-DFC-8CE1=	AS5350 Octal E1/PRI DFC card
AS535-DFC-60NP=	AS5350 60 Nextport DFC card
AS535-DFC-108NP=	AS5350 108 Universal Port Card
Cisco AS5350 Spare Accessories	
AS5350RM-19/24=	AS5350 19/24 Rack Mount Kit, Spare
AS535-FTA=	AS5350 Fan Tray Assembly, Spare
AS535-AC-PWR=	AS5350 AC Power Supply, Spare
AS535-DC-PWR=	AS5350 DC Power Supply, Spare
AS535-DFC-CC=	AS5350 DFC Carrier Card

1. This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco AS5350 Universal Gateway Web site: **http://www.cisco.com/go/as5350**

Cisco AS5400 Series Universal Gateways

Cisco AS5400 Series Universal Gateways offer unparalleled capacity in only two rack units (2RUs) and provides universal port data, voice and fax services on any port at any time. High-density (up to 1 CT3), low power consumption (7.2A at 48 VDC per CT3), and universal port digital signal processors (DSPs) make Cisco AS5400 Series Universal Gateways ideal for many network deployment architectures, especially colocation environments and mega points of presence (POPs).

The Cisco AS5400 Series consists of two models, the Cisco AS5400 and the Cisco AS5400HPX. The gateways share the same architecture; the primary difference is the processing capability of the two platforms. The Cisco AS5400 offers unparalled dial capacity and scalability for MLPPP, L2TP, and V.120 sessions, whereas the Cisco AS5400HPX provides enhanced performance for processor intensive voice and fax applications.

Cisco AS5400 Series support a wide range of IP-based value-added services such as high-volume Internet access, regional/branch-office connectivity, corporate virtual private networks (VPNs), mobile wireless solutions, long distance for Internet service providers (ISPs), international wholesale long distance, distributed prepaid calling, Signaling System 7 (SS7) interconnect, and enhanced voice services.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco AS5400HPX	• High density in a small footprint (16 CT1/CE1 or 1 CT3) • Universal port services (data, voice, fax) • Enhanced performance for processor intensive voice and fax applications • Compact form factor—easy to add capacity as the network grows • Low power per port • High performance async/ISDN/VoIP/wireless • T.38 real-time fax relay, T.37 fax store and forward, fax detection, unified communications • Flexible redundant backhaul methods
Cisco AS5400	• Async/ISDN/Wireless data to 1 CT3 • Universal port services (data, voice, fax) or voice only services to 16 CT1/CE1

Key Features

- The Industry's only 2RU, CT3-capable universal gateway on the market with hot-swappable cards, internal redundant power supply
- Universal Gateway which provides universal port data, voice, and fax services on any port at any time
- Feature cards: 8 or 16 CT1/CE1 feature cards; 60 or 108 channel Universal Port feature card; All feature cards and fan trays are hot-swappable
- Redundant 10/100 Ethernet ports and redundant 8 Mbps serial backhaul ports for Frame Relay, HDLC or PPP WAN Backhaul
- One fast console port for local administrative access; one auxiliary port for remote administrative access
- Redundant LAN/WAN backhaul ports
- ETSI/NEBS Level 3 compliant
- AC or DC power supply with dual fans
- Cisco SS7 signaling gateway interoperability

Competitive Products

• 3Com/CommWorks: Total Control C1000	• Lucent: Max TNT
• Alcatel: 7505 Series	• Siemens: HiPath Series

Specifications

Processor Type	Cisco AS5400HPX: 390-MHz RISC processor Cisco AS5400:250-MHz RISC processor
Calls Supported	Cisco AS5400HPX: Voice or universal port services - to 648 concurrent calls (to 20T1s/16E1s) or Remote access services - to 648 calls (to 1CT3/16E1s) Cisco AS5400: Voice or universal port services - to 480 concurrent calls (to 20T1s/16E1s) or Remote access services - to 648 calls (to 1CT3/16E1s)
SDRAM	256 MB (default), 512 MB (maximum)
Boot Flash	8 MB (default) 16 MB (maximum)
System Flash	32 MB (default) 64 MB (maximum)
Layer 3 Cache	Cisco AS5400HPX: 8 MB Cisco AS5400:2 MB
Shared input/output (I/O)	64 MB (default) 128 MB (maximum)
Feature Slots	7
Trunk Feature Cards	8 T1/E1/PRI 1 CT3
DSP Feature Card	60/180 Universal ports
LAN Protocols	IP, IPX, AppleTalk, DECnet, ARA, NetBEUI, bridging, HSRP, 802.1Q
WAN Protocols	Frame Relay, PPP, HDLC (leased line)
Routing Protocols	RIP, RIPv2, OSPF, IGRP, EIGRP, BGPv4, IS-IS, AT-EIGRP, IPX-EIGRP, Next Hop Resolution Protocol (NHRP), AppleTalk Update-Based Routing Protocol (AURP)
QoS Protocols	IP Precedence, Resource Reservation Protocol (RSVP), Weighted Fair Queuing (WFG), Weighted Random Early Detection (WRED), Multichassis Multilink PPP (MMP) fragmentation and interleaving, 802.1P
Access Protocols	PPP, Serial Line Internet Protocol (SLIP), TCP Clear, IPXCP, ATCP, ARA, NBFCP, NetBIOS over TCP/IP, NetBEUI over PPP, protocol translation (PPP, SLIP, ARA, X.25, TCP, LAT, Telnet), & XRemote
Bandwidth Optimization	Multilink PPP (MLPPP), TCP/IP header compression, Bandwidth Allocation Control Protocol (BACP), Bandwidth on demand, Traffic shaping

7629
3

Voice Compression	G.711, G.723.1 (5.3K and 6.3K), G.726, G.729ab, G.Clear, GSM-FR
DSP Voice Features	G.168 echo cancellation, programmable up to 128 ms Transparent transcoding between A-law and mu-law encoding Voice activity detection, silence suppression, comfort noise, fixed and adaptive jitter buffering Call progress tone detection and generation—Dial tone, busy, ring-back, congestion, and re-order tones, with local country variants Continuity Testing (COT) DTMF, MF
Voice and Fax Signaling Protocols	H.323v2, H.323v3, H.323v4, SIP, MGCP 1.0, TGCP 1.0, Voice Extensible Markup Language (VoiceXML), Real-Time Streaming Protocol (RTSP), Extended Simple Mail Transfer Protocol (ESMTP) T.37 fax store and forward T.38 real-time fax relay Fax detection Fax and modem passthrough Open Settlements Protocol (OSP) Media Recording Control Protocol (MRCP) Text to Speech (TTS) Servers Automatic Speech Recognition (ASR) Servers
SS7	Integrated SLT functionality
Network Security	RADIUS or TACACS+, PAP or CHAP authentication, local user/password database DNIS, CLID, call-type pre-authentication Inbound/outbound traffic filtering (including IP, IPX, AppleTalk, bridged traffic) Network Address Translation (NAT) and Dynamic access lists SNMPv2, SNMPv3
Virtual Private Networking	IP Security (IPSec) and Policy enforcement (RADIUS or TACACS+) L2TP, Layer 2 Forwarding (L2F), and generic routing encapsulation (GRE) tunnels Firewall security and intrusion detection
Channelized T1	Robbed-bit signaling; loop start, immediate start, and wink start protocols
Channelized E1	CAS, E1 R1, E1 R2, leased line, Frame Relay, G.703, G. 704
ISDN Protocols Supported	Sync mode PPP, V.120, V.110 at rates up to 38400 bps Network- and User-side ISDN DoVBS QSIG NFAS with backup D-channel
Modem Protocols Supported	V.90 or V.92 standard supporting rates of 56000 to 28000 in 1333 bps increments V.92 Modem on Hold, Quick Connect V.44 Compression Fax out (transmission) Group 3, standards EIA 2388 Class 2 and EIA 592 Class 2.0, at modulations V.33, V.17, V.29, V.27ter, and V.21 K56Flex at 56000 to 32000 in 2000 bps increments ITU-T V.34 Annex 12 at 33600 and 31200 bps and many others
Wireless Protocol	V.110, V.120
Full Cisco IOS Support	IP Plus and Enterprise Plus feature sets
Console and Auxiliary Ports	Asynchronous serial (RJ-45)
Chassis Dimensions (H x W x D)	3.5 x 17.5 x 18.25 in.
Chassis Weight (fully loaded)	35 lb maximum (15.8 kg)

For More Information

See the Cisco AS5400 Universal Gateways Web site: **http://www.cisco.com/go/as5400**

Cisco AS5850 Universal Gateway

The Cisco AS5850 Universal Gateway is a high-density, carrier-class gateway, offering unparalleled capacity and high availability. The Cisco AS5850 is specifically designed to meet the demands of large, innovative service providers, supporting up to five channelized T3s (CT3s), 96 T1s or 86 E1s of data, voice, and fax services on any port at any time. It offers high availability features such as hot-swap on all cards, load-sharing and redundant hot-swappable power supplies, redundant route processing cards and call admission control to ensure 99.999-percent availability.

The Cisco AS5850 supports a wide range of IP-based value-added services such as high-volume Internet access, corporate virtual private networks (VPNs), long distance for Internet service providers (ISPs), international wholesale long distance, distributed prepaid calling, Signaling System 7 (SS7) interconnect, and managed voice services such as hosted IP telephony, managed IP-PBX, multiservice VPNs, and IP contact centers.

Using the rich set of Cisco IOS Software features and Signaling System 7 (SS7) interconnection, service providers can quickly provision their network for new services to meet the rapidly changing demands of the communications provider marketplace.

As a highly flexible voice gateway, the Cisco AS5850 supports any coder-decoder (CODEC) at 100-percent capacity simplifying network engineering. An open programmable architecture streamlines rapid voice service creation with H.323, Session Initiation Protocol (SIP) or Media Gateway Control Protocol (MGCP).

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco AS5850	• Supporting up to 5 x CT3s, 96 T1s or 86 E1s of multiple data, voice, and fax services on any port at any time • Service provider or IP-focused installations • Highly available single system with multiple redundancy • Wholesale dial/voice, retail dial/voice, TDM grooming or wireless applications

Key Features

- High scalability—up to 3360 ports in a 14 RU chassis and provides for 6 times growth in same chassis
- Hot-swap redundant power supplies and power feeds
- Redundant DSPs and RSC
- Thermal/Power management and redundant fans
- DSP Resource Recovery Feature
- Supports H.323v2, H.323v3, H.323v4, SIP and MGCP 1.0
- Application-specific support including AOL and Prodigy traffic
- WAN optimization including routing filters, snapshot routine, dial-on-demand routing ASAP
- ETSI/NEBS Level 3 compliant
- Cisco SS7 signaling gateway interoperability

Competitive Products

- 3Com: TC 2000
- Lucent: APX 8000
- Siemens: HiPath Series
- Alcatel: 7505 Series

Specifications

Feature	Cisco AS5850
Slots	12 feature board slots 2 RSC slots
Processor Type	266 MHz RISC processor plus 2MB of L3 cache SDRAM
RSC Switch Fabric	5 GBps, Layer 3 / 4 switching
Memory	512 MB SDRAM with ECC per RSC 128 MB SDRAM (with parity) per feature card
Trunk Cards	Single CT3 plus 216 DSP Channel feature card 24 CE1/CT1 feature card G.703, G.704
Universal Port Card	324 Channel DSP-feature card
Egress Ports	Dual Gigabit load-balanced redundant Ethernet ports with GBIC interfaces for user traffic One 10/100-Mbps Ethernet port with RJ45 connector for management traffic
LAN Protocols	IP
Service Support	Port Policy Management and SS7/C7
Routing Protocols	RIP, RIPv2, OSPF, IGRP, EIGRP, BGPv4, IS-IS, Next Hop Resolution Protocol (NHRP)
Access Protocols	PPP, Serial Line Iternet Protocol (SLIP), TCP Clear
Bandwidth Optimization	Multilink PPP (MLPPP), TCP/IP header compression, Bandwidth Allocation Control Protocol (BACP), Bandwidth on demand, Nonfacility-associated signaling (NFAS),traffic shaping
Network Security	RADIUS or TACACS+, PAP or CHAP authentication, local user/password database, DNIS, CLID, call-type pre-authentication, Inbound/outbound traffic filtering (including IP), SNMPv2, SNMPv3
Virtual Private Networking	IP Security (IPSec) and Policy enforcement (RADIUS or TACACS+), L2TP, Layer 2 Forwarding (L2F), and generic routing encapsulation (GRE) tunnels, Firewall security and intrusion detection, IP Precedence, policy-based routing
Channelized T1	PRI, robbed-bit signaling; loop start, immediate start, and wink start protocols
Channelized E1	CAS, E1 R2, PRI
ISDN Protocols	Sync mode PPP, V. 120, V. 110 at rates up to 38400
Voice Protocols	G.711, G.723.1, , G.726, G.729ab, G.Clear, GSM-FR H.323v2, H.323v3, H.323v4, SIP, MGCP 1.0 ECAN up to 128ms T.38 real-time fax relay Fax detection Fax and modem passthrough
Modem Protocols	V.90 or V.92 standard supporting rates of 56000 to 28000 in 1333-bps increments V.44 supporting increased throughput by more than 100 percent for Internet browsing Fax out (transmission) Group 3, standards EIA 2388 Class 2 and EIA 592 Class 2.0, at modulations V.33, V.17, V.29, V.27ter, and V.21 K56Flex at 56000 to 32000 in 2000-bps increments ITU-T V.34 Annex 12 at 33600 and 31200 bps and more
ISDN Protocols	Sync mode PPP, V.120, V.110 at rates up to 38400 bps
Wireless Protocol	V.110
Console and Auxiliary Ports	Asynchronous serial (RJ-45)
Chassis Dimensions (HxWxD)	24.5 x 17.5 x 24 in.
Chassis Weight	220 lb (100 kg)

For More Information

See the Cisco AS5850 Web site: **http://www.cisco.com/go/AS5850**

Remote Dial Access Network Management Products

Universal Gateway Manager (UGM)

Network management applications and tools are critical for the successful deployment and operations of voice or data services. The Cisco Universal Gateway Manager (UGM) is an element management system for Cisco AS5000 Universal Gateways. The Cisco UGM enables network operators and administrators to efficiently deploy, manage and maintain Cisco AS5000 Universal Gateways supporting Voice over IP, managed voice, PSTN gateway, and dial access services.

Key Features

- Enables the efficient deployment and configuration of Cisco AS5000 Universal Gateways
- Monitors the operational status of Cisco AS5000 Universal Gateways and their subcomponents so that corrective action can be taken quickly
- Supports the rapid reconfiguration of Cisco AS5000 Universal Gateways for network or service changes
- Collects and presents a wide range of performance-related statistics for monitoring gateway and network efficiency
- Co-resides with Cisco MGC Node Manager (MNM) for Cisco PGW 2200 PSTN Gateway node management
- Provides interfaces to support its integration with existing network management applications

For More Information

See the Cisco Universal Gateway Manager Web site: **http://www.cisco.com/go/ugm**

Cisco Universal Gateway Call Analyzer

The Cisco Universal Gateway Call Analyzer (UGCA) tool monitors and troubleshoots Cisco AS5000 universal gateways that support dialup services. The Cisco Universal Gateway Call Analyzer complements other network management system (NMS) applications, adding call-level analysis capabilities that are not available with standard NMS applications.

Maintaining high call-success rates and quality connections are key challenges for any dial service provider. These metrics directly affect customer satisfaction and are fundamental indicators of network performance and efficiency. Numerous issues may cause service degradation, which may be rapid or may occur slowly. While public switched telephone network (PSTN) issues are frequently the source of problems, they are especially difficult to identify.

Cisco AS5000 universal gateways collect the detailed call-characteristic data needed to detect and diagnose issues that affect service. The Cisco Universal Gateway Call Analyzer is the window into this data, providing analysis and reporting features through an intuitive Web interface.

For More Information

See the Cisco Universal Gateway Call Analyzer Web site:
http://www.cisco.com/go/ugca

Cisco Resource Policy Management System

Wholesalers face a challenge when delivering service level agreements (SLAs) on a common network, especially when providing a range of services for different customers. The Cisco Resource Policy Management System (RPMS) is a software tool that provides policy management of platform resources. With Cisco RPMS, wholesalers are able to offer a variety of services to a variety of customers on a single set of gateways. Cisco RPMS offers not only effective resource management but the capability to build and deliver flexible service models that fit customers' unique requirements. Cisco RPMS can grow to support a wholesaler's changing needs, scaling as the network expands and delivering the services that customers demand, including wholesale dial, access to virtual private network (VPN) services.

Selected Part Numbers and Ordering Information[1]

Resource Policy Management System	
FR5X-PM-LIC	Port management license for 1 port (includes Resource Pool Manager, Call Tracker)
CRPMS-2.0	Cisco Resource Pool Manager Server v2.0 (1 server)
CRPMS-2s-2.0	Cisco Resource Pool Manager Server v2.0 (2 servers)
CRPMS-6S-2.0	Cisco Resource Pool Manager Server v2.0 (6 servers)
CRPMS-UPGRADE-2.0	Single Server Upgrade License from RPMS 1.x to version 2.0

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco Universal Gateway Manager: **http://www.cisco.com/go/ugm**
See the Resource Pool Manager Web site: **http://www.cisco.com/go/rpms**

SS7 Signaling & Softswitch Products

Cisco AS5x00 series products interoperate with various SS7 and Softswitch products, including the Cisco SC2200 Signaling Controller, the Cisco PGW 2200 Softswitch and the Cisco BTS 10200 Softswitch.

Cisco SC2200 Signaling Controller

Please see PGW 2200 Softswitch.

Cisco PGW 2200 Softswitch

The Cisco PGW 2200 provides the signaling and call control functionality that enables service providers (SPs) to bridge the boundary between the legacy PSTN and today's new world packet networks. Combined with Cisco's award winning media gateways, the PGW 2200 is the catalyst for PSTN Gateway solutions enabling dial offload, transit, business voice, H.323 and SIP based applications. The PGW 2200 leverages its protocol library of 90+ SS7/C7 variants to enable interconnect worldwide. In signaling mode the PGW adds SS7/C7 to the AS5X00 gateways, giving service providers around the world a proven cost-saving and reliable solution for connecting VoIP and Internet Dial Access solutions to the PSTN. SS7 signaling allows service providers to enter into new markets, optimize their networks for both voice and data traffic, and save drastically on monthly interconnect fees.

Cisco BTS 10200 Softswitch

The Cisco BTS 10200 Softswitch provides call-control intelligence for establishing, maintaining, routing, and terminating voice calls. The Cisco BTS 10200 Softswitch also serves as an interface to enhanced service and application platforms. Leveraging the power of packet networks while seamlessly operating with legacy circuit switched infrastructures, the Cisco BTS 10200 Softswitch empowers service providers and carriers to gracefully transition to packet-based technology. Implementing the Cisco BTS 10200 Softswitch ensures rapid service deployment, carrier-grade reliability, service flexibility, scalability to millions of subscribers, and cost savings through investment optimization and operational efficiencies.

For More Information

See SS7 Signaling & Softswitch Products Web site:
http://www.cisco.com/en/US/products/hw/vcallcon/index.html

Additional Remote Dial Access Products

- In addition to the AS5350/AS5400/AS5850 series access gateways, the Cisco 2600/3600 series routers (see pages 1-16 and 1-22) also support dial-up, data, and voice access via network and modem modules, and voice interface cards
- For sites that require access via multiple external analog modems, the AS2509/AS2511-RJ access servers (see page 1-14) and 2600 series routers (see page 1-16) are ideal for low-density, dial applications
- For small office ISDN connectivity, see Cisco 800 series routers (see page 1-9)

Cisco uBR7100 Series Universal Broadband Router

The Cisco uBR7100 Series is a complete, compact, easy-to-use product that enables cost-effective, high-speed Internet access in the hospitality multidwelling (MDU) and multitenant (MTU) market space using the coaxial cable already in a building. The product requires exceptionally low capital investment and minimal setup time to provide online Internet access and support residential voice services. For Tier 2 or Tier 3 cable operators, it is the industry's most cost-effective, feature-rich CMTS and integrated router. The Cisco uBR7111 and Cisco uBR7114 models are CableLabs qualified to DOCSIS 1.0 specifications. The Cisco uBR7111E and Cisco uBR7114E models are tComLabs qualified to EuroDOCSIS 1.0 specifications. The Cisco uBR7111 and Cisco uBR7111E contain one downstream port and one upstream port. The Cisco uBR7114 and Cisco uBR7114E contain one downstream port and four upstream ports. All models support bidirectional or telco-return traffic.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco uBR7100 Series	• For MxU customers: the Cisco uBR7100 Series enables high-value Internet and residential voice services over a DOCSIS or EuroDOCSIS cable infrastructure • For cable operators: the Multi-tenant/dwelling Unit (MxU) market represents an untapped opportunity to expand broadband cable service. Given the small subscriber base of a typical MxU setting, the challenge has been to deliver robust services quickly and cost-effectively for an accelerated break-even point and a quicker return on investment—enabled by the Cisco uBR7100 Series

7623 3

Key Features

- Complete package that includes a combined router and CMTS with an integrated upconverter, and embedded Network Interface
- Standards-based: DOCSIS 1.0 and DOCSIS 1.1-based; EuroDOCSIS models available
- Reliable operation to ensure the system remains online
- Uses Cisco IOS Software

Specifications

Feature	Cisco uBR7111 and uBR7114	Cisco uBR7111E and uBR7114E
Memory	Flash: 48 MB; System: 128 MB	Flash: 48 MB; System: 128 MB
Line Card with Integrated Upconverter (Cable Plant Interface)	uBR7111: 1 downstream and 1 upstream uBR7114: 2 downstream and 4 upstreams	uBR7111E: 1 downstream and 1 upstream uBR7114E: 2 downstream and 4 upstreams
Integrated Upconverter	DOCSIS Annex B, 6 MHz High level output: =+61dBmV, 55 to 858 MHz Optimized for 64 and 256 QAM	DOCSIS Annex A, 8 MHz, High level output: = +61 dBmV, 55 to 858 MHz Optimized for 64 and 256 QAM
Port Adapter (WAN or backbone Interface)	Embedded dual 10/100 BaseT Ethernet (TX FE) provided Supports one additional PA; options include the following using Cisco IOS Release12.1(8)EC minimum: Ethernet: • PA-4E-4-port Ethernet 10BASE-T • Fast Ethernet: • PA-FE-TX-1-port 100BASE-TX Fast Ethernet • PA-FE-FX-1-port 100BASE-FX Fast Ethernet • PA-2FE-TX 2-port 100BASE-TX Fast Ethernet • PA-2FE-FX 2-port 100BASE-FX Fast Ethernet Serial: • PA-MC-4T1 4-port multichannel T1 Port Adapter with integrated CSU/DSUs • PA-MC-2T1 2-port multichannel T1 Port Adapter with integrated CSU/DSUs • PA-E3-1-port E3 serial Port Adapter with E3 DSU • PA-T3-1-port T3 serial Port Adapter with T3 DSU • PA-2E3-2-port E3 serial Port Adapter with E3 DSUs • PA-2T3-2-port T3 serial Port Adapter with T3 DSUs • PA-4T+-4-port serial Port Adapter, enhanced • PA-4E1G-75-4-port E1-G.703 serial Port Adapter (75-ohm/unbalanced) • PA-4E1G-120-4-port E1-G.703 serial Port Adapter (120-ohm/balanced) HSSI: • PA-2H-2-port HSSI • ATM: • PA-A3-8T1IMA, 8-port ATM inverse T1 multiplexer Port Adapter • PA-A3-OC3SML—1-port OC-3c ATM, PCI-based single-mode long reach port adapter • PA-A3-OC3MM, 1-port ATM enhanced OC3c/STM1 multimode Port Adapter • PA-A3-OC3SMI—1-port OC-3c ATM, PCI-based single-mode intermediate reach port adapter POS: • PA-POS-OC3SMI, 1-port Packet/SONET OC3c/STM1 single-mode Port Adapter	Same as Cisco uBR7111 and Cisco uBR7114

Feature	Cisco uBR7111 and uBR7114	Cisco uBR7111E and uBR7114E
Power Options	Single; 100 to 240 VAC input voltage	Single; 100 to 240 VAC input voltage
Minimum Cisco IOS Software Release	12.1(5)ECI minimum	12.1(7)EC minimum

For More Information

See the Cisco uBR7100 series Web site: **http://www.cisco.com/go/ubr7100**

Cisco uBR7246VXR Universal Broadband Router

The Cisco uBR7246VXR-a member of the Cisco uBR7200 Series-combines the functionality of a CMTS with an advanced router. The Cisco uBR7246VXR provides a single, multiservice, scalable platform that gives cable companies and ISPs the ability to deliver IP data and VoIP services to DOCSIS or EuroDOCSIS-compliant cable modems and set-top boxes. The Cisco uBR7246VXR is CableLabs qualified to DOCSIS 1.1, as well as PacketCable 1.0 specifications. The product is also tComLabs qualified to EuroDOCSIS 1.1 specifications.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco uBR7246VXR	• Positioned for high-growth cable deployments • Flexible port expansion for multiservice deployment options • Supports up to 8,000 subscribers per chassis with 3.2 Gbps back plane • 4 line card slots, 2 port adapter slots, 1 I/O controller slot, 1 NPE slot, and 1 clock card slot for VoIP

Key Features

- Standards-based—Supports DOCSIS/EuroDOCSIS 1.0 and DOCSIS 1.1
- Modularity allows for customized configuration per plant characteristics for optimization of topology and network bandwidth
- Cisco IOS Software—Delivers proven stability and offers advanced features such as multiprotocol routing, tunneling, bandwidth management, QoS, guaranteed service levels, service-level monitoring and many CPE management options
- Ease of management and upgrades—Supports online insertion and removal of components to allow seamless upgrades of port adapters, line cards, and power supplies without service interruption. Provides single, centralized point of administration for remote devices

Specifications

Feature	Cisco uBR7246VXR
Cable Line Cards and Number of Slots	4
Supported cable line cards (Cable Plant Interfaces)	uBR-MC14C; uBR-MC16C; uBR-MC16E; uBR-MC16S; uBR-MC28C
Port Adapter Slots (LAN/WAN interfaces)	2
Supported PA categories	Ethernet: Fast Ethernet; Gigabit Ethernet Serial (V.35, E1-G.703/G.704, T3/E3) Serial Multi-channel T1 HSSI ATM T3/E3 ((PCI-based) ATM OC-3c (PCI-based) POS OC-3c DPT OC-12c/STM4c
Power Supply Shots	2
Power Supply Option	AC; Dual AC; DC; Dual DC

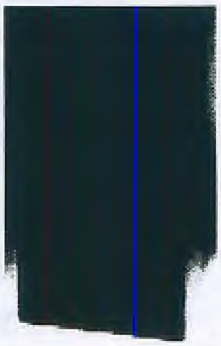
Feature	Cisco uBR7246VXR
Input/Output (I/O) controller	uBR7200-I/O uBR7200-I/O-FE uBR7200-I/O-2FE/E
I/O flash options for PCMCIA slots	Flash disk (48 MB) Flash disk (128 MB)
Network processing engines (NPE)	uBR7200-NPE-G1,NPE-400, and NPE-225
Add-on processor memory options	SDRAM (128 MB, 256 MB) for NPE-225 only SDRAM (128 MB, 256 MB = 512 MB) for NPE-400 only 1 GB, 512 MB, 128 MB for uBR7200-NPE-G1
Router Bandwidth	3.2 Gbps

7621
ε

For More Information

See the uBR7200 Web site: **http://www.cisco.com/go/ubr7200**

Cisco uBR10012 Universal Broadband Router



The Cisco uBR10012 Universal Broadband Router is a new class of CMTS, that handles the volume, capacity, and complexity of large cable headends or distribution hubs. It combines the revenue-generating features and stability of the market-leading Cisco uBR7200 Series with an architecture that is optimized for aggregation and virtually limitless future growth. The Cisco uBR10012 goes beyond the traditional "carrier class" definition, to deliver the highest level of service availability and capacity of any production CMTS available today. It employs a mix of distributed, centralized, and parallel processing to enable consistently high, real-world performance. The Cisco uBR10012 is CableLabs qualified to DOCSIS 1.0 and DOCSIS 1.1 specifications. The product is also tComLabs qualified to EuroDOCSIS 1.0 specifications.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco uBR10012	• High-end throughput, capacity, and service handling for a mix of IP data, voice, and video services over cable—supporting a wide variety of applications, media, session types, subscriber profiles, and access devices • Support for advanced feature sets, varying QoS requirements, service-level differentiations, and transport strategies (MPEG, IP, multicast, unicast, broadcast) that include implementing flow control to various cable CPE devices

Key Features

- Highest-capacity CMTS that leverages the proven stability of the industry-standard Cisco uBR7200 Series, the highly scalable architecture of the Cisco 10000 Internet Router, and feature-rich Cisco IOS Software
- Multiservice support, optimized to provide high throughput and accelerated processing using PXF technology; exceptional throughput on each connection in the chassis is achieved
- Standards-based design, support includes DOCSIS 1.0 and DOCSIS 1.1
- Reliability—Designed to eliminate single points of failure and allow technicians to swap out cards online; architected to provide redundancy throughout the system that includes redundant processing engines, bus interconnects, and power supplies

- Secure, scalable choices protect your investment and ensure current and future business growth can be accommodated; the architecture supports planned system and network expansion, including scaling IP services forwarding capacity, increasing connection speeds and densities, and extensive route scaling techniques

Specifications

Feature	Cisco uBR10012
Modular Slots	8 slots for cable line cards 4 slots for LAN/WAN interfaces 2 slots for Performance Routing Engines (PREs) 2 slots for Timing Communication and Control Plus (TCC+) modules
Supported Cards	Cable line cards that include: Cisco uBR line cards with a Cisco Line Card Processor (LCP2) and Cisco 5X20 BPE Timing, Communications, and Control Plus (TCC+) card Gigabit Ethernet (GE) network uplink card OC-12 Packet Over SONET (POS) network uplink card OC-48 DPT Interface
Processor Type	Parallel Express Forwarding (PXF)
Flash Memory	48 MB (default); 128 MB (maximum)
DRAM Memory	512 DRAM (default)
Software Supported	Minimum software requirement: Cisco IOS Software Release 12.2(11)BC1 minimum for the Cisco 5X20 BPE, Cisco IOS Software Release 12.2(13)BC minimum for the Cisco OC-48 DPT Interface
Power Supply	DC, AC
Hot-Swappable	Yes
Backplane Capacity	51.2 Gbps
Physical Dimensions (H x W x D)	Height: 31.25 in. (79.4 cm)—18 rack units (RU) Width: 17.2 in. (43.7 cm) Depth: 22.75 in. (57.8) Mounting: 19 in. rack mountable (front or rear), 2 units per 7 ft. rack Note: Mounting in 23 in. racks is possible with optional third-party hardware
Weight	Weight: 235 lb (106.6 kg) fully configured chassis

For More Information

See the Cisco uBR10012 Web site: **http://www.cisco.com/go/ubr10012**

Cisco RF Switch

The Cisco RF Switch works with the Cisco uBR10002 and uBR7246VXR Universal Broadband Router to provide a fully redundant DOCSIS system that enables cable service providers to achieve PacketCable system availability, minimize service disruptions, and simplify operations. The Cisco RF Switch is part of Cisco's newest high-availability N+1 solution set. In combination with the Cisco uBR10012 and uBR7246VXR, the Cisco RF Switch enables a fully redundant CMTS with no single point of failure. The product maximizes density with more than 250 MCX-type connectors that interface the Cisco uBR10012 and the cable plant. The Cisco RF Switch contains RF combiners/splitters, RF switch logic, and RF switch drivers. The product offers ten upstream switch modules, three downstream switch modules, an Ethernet controller module, an AC or DC power supply, and color coding, preterminated cabling.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco RF Switch	As cable service providers enter the VoIP market, high availability (24x7 service) for broadband cable IP services is becoming a requirement. The Cisco RF Switch enables cable service providers to achieve PacketCable system availability, minimize service disruptions, and simplify operations.

Key Features

- Front-panel serviceability with module Hot Swap capability that eliminates downtime for RF paths
- Modular upstream and downstream capacity with ten upstream, three downstream, and one blank slot that optimizes the serviceability of the CMTS; each of the 14 modules represent a port on a cable line card. Each switch module contains seven working or "active" inputs, plus one protect or "standby" input and seven protected outputs. Inputs are connections from the Cisco uBR10012 and uBR7246VXR to the Cisco RF Switch. Outputs are connections from the Cisco RF Switch to the HFC plant
- Fully passive working path; hardware components do not affect data and VoIP services
- Active components only in protect path; servicing of protect cards offer no disruption to data and VoIP services
- Position-sensing latching relays; robust design maintains operation during power disruptions
- Flexible, external design with more than 250 connectors—unmatched port density
- N+1 redundancy

Specifications

Feature	Cisco RF Switch
Input Power Requirements	• AC: 100 to 240 VAC, 50 or 60 Hz, operating range: 90 to 254 VAC • DC: -48 to -60 VDC, operating range: -40.5 to –72 VDC, 200 mVpp ripple/noise
Environmental	• Operational temperature range: 0 to +40°C • Operating temperature range: -5 to +55°C
Unit Control	• 10BaseT Ethernet—SNMP • Switching time from active (working) to standby (protect): 150 mS maximum after SNMP command • Cisco uBR10012 and uBR7246VXR
Connectors	• RF connectors: MCX • AC power: IEC320 type • DC power: Three terminal block • Ethernet: RJ-45 • RS-232 Bus: 9-pin male D
Reliability	• 41,000 MTBF @ +50°C as calculated by Bellcore 5, 80 percent confidence factor
Physical	• Dimensions (H x W x D): 19 x 15.5 x 5.25 in. (842 x 384 x 132 mm) • Weight: 36 lbs
Input Power Requirements	• AC: 100 to 240 VAC, 50 or 60 Hz, operating range: 90 to 254 VAC • DC: -48 to -60 VDC, operating range: -40.5 to –72 VDC, 200 mVpp ripple/noise

Feature	Cisco RF Switch
Environmental	• Operational temperature range: 0 to +40°C • Operating temperature range: -5 to +55°C
RF requirements	• Input/output impedance: 75 ohms • Maximum RF input power: +15 dBm (63.75 dBmV) • Switch type: Electro-mechanical, absorptive for working path, non-absorptive on the protect path • Switch setting time per switch module: 20 ms maximum • Downstream frequency range: 54 to 860 MHz • Typical downstream insertion loss: +/-1.1 dB from CMTS to cable plant; +/- 2.1 dB from protect to cable plant; 5.5 dB from working to output; 8.0 dB from protect to output • Downstream insertion loss flatness: +/- 1.1 dB from CMTS to cable plant; +/- 2.1 dB from protect to cable plant • Downstream output return loss: >15.0dB at <450 MHz, > 12.0 dB at >= 450 MHz • Downstream input return loss: >15.0 dB • Downstream isolation: > 60 dB from channel to channel in working mode; > 52 dB from CMTS to protect when in protect mode • Upstream frequency range: 5 to 70 MHz • Typical upstream insertion loss: 4.1 dB from cable plant to CMTS; 5.2 dB from cable plant to protect • Upstream insertion loss flatness: +/- 0.4 dB from cable plant to CMTS, +/- 0.6 dB from cable plant to protect • Upstream input return loss:> 16 dB • Upstream isolation: > 60 dB from channel to channel in working mode; > 60 dB from CMTS to protect when in protect mode • Protect mode: CMTS return loss >10 dB, cable plant return loss: >10dB

7618

For More Information

See the Cisco RF Switch Web site: **http://www.cisco.com/go/rfswitch**

Broadband Cable—Customer Premise Equipment (CPE)[1]

Cisco uBR900 Series Cable Access Routers

The Cisco uBR900 Series Cable Access Routers provide commercial services for cable operators, allowing them to expand their broadband service offerings. Both the Cisco uBR905 and Cisco uBR925 support IP data transmission over a cable plant and offer hardware-accelerated IPSec VPN support.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco uBR905 Cable Access Router	• Data-only broadband services (or voice separately via Ethernet) • High-speed, secure remote tunneling via hardware accelerated IPSec VPN
Cisco uBR925 Cable Access Router	• Two voice (VoIP) connections via RJ-11 ports • Data broadband services, router functionality, and VPN support • Easy-to-manage solution for telecommuters and small offices

[1] Cisco VoIP Residential CPE Partner Program—To help drive deployment of residential VoIP services to market, Cisco offers a program that identifies low-cost residential VoIP modems that have passed interoperability testing with Cisco. Cable service providers should contact their sales representatives for vendors, models, pricing and volume discount opportunities.

Key Features

- Integrated high-speed cable modem and router that operates with any DOCSIS 1.1 or DOCSIS 1.0-compliant CMTS; both Cisco uBR900 Series models are DOCSIS 1.1-ready
- Integrated Cisco IOS Software router, cable modem, and four-port Ethernet hub that offers advanced networking capabilities and investment protection

Specifications

Feature	Cisco uBR905	Cisco uBR925
Ports	4-port 10Base-T Ethernet hub 1-port console 1-port CATV (Female F Connector)	4-port 10Base-T Ethernet hub 1-port USB 2 ports RJ-11 1-port console 1-port CATV
Routing Features	NAT/PAT, DHCP Server	Same as Cisco uBR905
Security Features	56-bit IPSec 3DES IPSec optional IPSec hardware acceleration Firewall optional	Same as uBR905
Voice Support	No	Yes

For More Information

See the uBR900 series Web site: **http://www.cisco.com/go/ubr900**

Remote Cable Access—Network Management Products

Cisco Cable Manager

Cisco Cable Manager is a client/server application that helps cable service providers deploy, maintain, monitor and troubleshoot cable equipment on an HFC network. The product manages DOCSIS and EuroDOCSIS-compliant CMTS and CPE, providing both operations center visibility, as well as technician access.

Cisco Cable Diagnostic Manager

Cisco Cable Diagnostic Manager is a web-based tool to help Customer Service Representatives at cable companies better handle subscriber calls and determine where problems reside in the network. Cisco Cable Diagnostic Manager provides status summary for the network neighborhood and fiber node, status on the DOCSIS or EuroDOCSIS-certified cable modem, as well as status on the Cisco CMTS products: Cisco uBR10012, uBR7200 Series, and uBR7100 Series.

Cisco Broadband Troubleshooter

Cisco Broadband Troubleshooter provides an efficient tool to help network operations center (NOC) personnel and field technicians detect, diagnose, and isolate problems between the cable plant and connected DOCSIS CPE devices. The product allows a technician to characterize upstream and downstream trouble patterns and quickly identify "flapping" CPE devices that are experiencing persistent connectivity problems. Operators can quickly discern CPE connectivity impairments by identifying noise, attenuation, provisioning, and packet-corruption issues.

Cisco Broadband Configurator

Cisco Broadband Configurator is a GUI-based tool designed to collect information needed to generate and download configuration files for DOCSIS or EuroDOCSIS cable modems and set-top boxes. There are two versions of the tool: a free, web-based version accessible via Cisco.com, and a stand-alone Java-based desktop version. Cisco Broadband Configurator enables point and click configuration of CPE values for RF, class of service, vendor information, SNMP parameters, BPI, TFTP, telco-return attributes, and CPE data.

For More Information

See the Cable Manager Web site: **http://www.cisco.com/go/cablemgr**
See the Cisco Cable Troubleshooter Web site:
http://www.cisco.com/go/troubleshooter

DSL Remote Access—Customer Premise Equipment (CPE)

Cisco offers the industry's broadest array of business-class DSL (G.SHDSL and ADSL) CPE solutions, from Enterprise to branch office, to Small Office/Home Office (SOHO) applications. Cisco's CPE solutions offer the choice of key features including Firewall, VPN, and Voice-over DSL support. And, Cisco's industry leading IOS-based capabilities enable QoS, policy management, and standardized set-up and configuration. Cisco CPE Products include:

- Cisco SOHO Series Ethernet, ADSL over ISDN, ADSL and G.SHDSL RoutersRouters (page 1-8)
- Cisco 800 Series Routers (page 1-9)
- G.SHDSL WAN Interface Cards (WICs) for 1700, 2600/2600XM, 3600 Series (see
  Chapter 1: Routers)
- Cisco IAD 2400 Series (w/G.SHDSL) (page 4-21)

Broadband Services Aggregation

The Cisco broadband aggregation portfolio includes the Cisco 6400 Broadband Aggregator, Cisco 7200 Series Router, the Cisco 7400 Series Internet Router, and the Cisco 10000 Series Internet Router. This portfolio covers all possible broadband aggregation markets. The Cisco 6400 and Cisco 10000 Series routers are carrier class broadband aggregation routers designed to provide high-density, high-performance services while maintaining the high-availability standards of large-scale carrier deployments. The Cisco 7200,Cisco 7301and Cisco 7400 Series routers cover the ISP and retail space by providing a dense, feature-rich platform but only taking a small footprint in the network.

- Cisco 7400: Highest density PPP aggregation per rack-unit
- Cisco 7301: Highest Density PPP aggregation per rack-unit
- Cisco 7200: Most versatile platform
- Cisco 6400: Only platform offering ATM switching and broadband aggregation
- Cisco 10000: Highest availability on a carrier-class integrated edge router

With this portfolio, Cisco can address the broadest set of requirements in terms of form factor, density, performance and scale, and offer customers a unique level of choice, with products optimized for any customer deployment.

Cisco 7200 Series

When ordered with the Cisco IOS 7200 Series Broadband User Services License (part number FR-BUS72), the 7200 delivers scaled PPP, RBE, and L2TP sessions and tunnels in addition to rich IP services. It enables service providers to provision broadband Internet access and supports all of the popular access technologies deployed today, including DSL, Cable, Wireless, and Dial Access. It is ideal for medium-density applications and is capable of handling up to 16000 subscribers in a single chassis. The 7200 is a modular platform with a choice of processing engines and a wide variety of WAN and LAN port adapters, including T1/E1, DS3, OC-3, Fast Ethernet, and Gigabit Ethernet. See page 1-31 for more information on the 7200 series.

Cisco 7301 Series

When ordered as 7301-BB-8K and 7301-BB-16K the Cisco 7301 Series Router provides a compact, high-performance single-rack-unit (1RU) router coupled with a broad set of interfaces and Cisco IOS® Software features, which makes it ideal for Broadband applications. The Cisco is capable of handling up to 16,000 simultaneous sessions and allowing for a pay-as-you-grow "rack and stack" architecture.

Cisco 7400 Series

When ordered as a part number 7401ASR-BB, the 7400 series provides high-performance broadband services aggregation like the 7200, but in a low-power one rack unit (1 RU) form factor. It offers one port adapter (PA) slot supporting over 40 standard 7200 series PAs, including T1/E1, DS3, OC-3, Fast Ethernet, and Gigabit Ethernet; making it ideal for small- and medium-density applications. See page 1-38 for more information on the 7400 series.

Cisco 10000 Series

With recent enhancements, the Cisco 10000 is the industry's only integrated edge router that delivers highly available, line-rate performance without compromises for service providers deploying IP services to broadband, leased line, ATM, and frame relay customers. With 99.999 percent uptime, the platform delivers high-performance broadband features including support for 32,000 (61,500 in the future) broadband subscribers, hardware-accelerated PPP over Ethernet and PPP over ATM, routed bridge encapsulation and 1483 routing. See page 1-47 for more information on the 10000 series.

Cisco 6400 Series

The Cisco 6400 is designed for use in high-availability environments such as service provider central offices, and corporate premises; and aggregates access media (DSL, cable, wireless, and dial) to serve as the intelligent equal access point, allowing multiple operating companies and service providers access to end users. It includes switch, router, and line card redundancy.

The Cisco 6400 is a high-performance service gateway that enables the delivery of network services, VPNs, and voice- and entertainment-driven traffic over any access media. ATM interfaces connect the Cisco 6400 to dial access servers, DSLAMs, and Cisco IP DSL Switches; ATM and packet interfaces connect to the network core.

Key Features

- Session scalability and modular design—The Cisco 6400 represents a quantum leap in session scalability, capable of scaling from 2000 subscribers in its entry level configuration to 96,000 subscribers in a full configuration.
- Routing and VPN scalability—Using the Cisco 6400, service providers can simultaneously route end-user traffic over secure, independent pathways exceeding 1000 different domains or end destinations, with an aggregate throughput of over 2.4 Gbps forwarding capacity for handling even the most bandwidth-intensive broadband traffic.

For More Information

See the 6400 series Web site: **http://www.cisco.com/go/6400**

ATM Multiservice WAN Switching

Cisco BPX 8600 Series—Advanced ATM Multiservice Switches

The Cisco BPX 8600 series is standards-based ATM switch with advanced IP and ATM capabilities. Designed to meet the demanding, high-traffic needs of a public service provider or large private enterprise, the BPX switch delivers high-performance ATM switching, multiservice adaptation and aggregation for all types of user traffic. Proven in the world's largest ATM and Frame Relay networks, the BPX 8600 enables service providers and large enterprises to meet skyrocketing network demands.

The Cisco BPX 8600 series switch offers up to 20 Gbps of high-throughput switching for multiple traffic types data, voice, and video and supports a wide range of interfaces, from Frame Relay to full broadband subscriber interfaces, up to 622 Mbps. You can offer multiple services for LAN, X.25, SNA, IP, Frame Relay, and ATM traffic from a single BPX platform. The Cisco BPX 8600 series supports multiprotocol label switching (MPLS) today, and this functionality can be easily added to any BPX switch already installed in the field.

For More Information

See the Cisco BPX Web site: **http://www.cisco.com/go/bpx**

Cisco MGX 8850 ATM Multiservice Switch

The Cisco MGX 8850 ATM Multiservice Switch enables delivery of a complete portfolio of service offerings while scaling from DS0 to OC-48c/STM-16 speeds. It enables service providers to be first to market with the new high-margin voice and data services while maintaining existing services.

The MGX 8850 universal chassis provides a unified ATM architecture that delivers a complete portfolio of differentiated services —from circuit emulation to IP VPNs—all with a single chassis, to enable service providers to easily add new services.

7613
ε

The Cisco MGX 8850 can function in three different modes of operation:

- PXM-1 configuration—Operates as a stand-alone device for narrowband services, or as an integrated edge concentrator for the Cisco BPX 8600 series or the Cisco MGX 8850 PXM-45
- PXM-1E configuration-Operates as a stand alone switch for low density narrowband services and included 1.2 Gbps switch card and PNNI routing
- PXM-45 configuration—Serves as a broadband edge switch and includes the 45 Gbps switch card and broadband ATM modules

Key Features

- Flexible ATM multiservice platform
- Highly scalable—from 1.2 to 45 Gbps of non-blocking throughput in single chassis
- Highest reliability, availability, and serviceability in the industry
- IP VPNs using Cisco IOS software-based Multiprotocol Label Switching (MPLS)
- Market-leading Frame Relay capabilities, with price-per-port leadership and advanced QoS
- High-density Point-to-Point protocol (PPP) for Internet access and aggregation
- Full-featured narrowband ATM for managed data, voice, and video services; high-density broadband ATM for wholesale ATM services
- Circuit Emulation for Private Line replacement
- Highly scalable packet voice gateway providing VoIP, VoATM(AAL1 & AAL2), ATM SVCs, Onboard MPLS

For More Information

See the Cisco MGX 8850 Web site: **http://www.cisco.com/go/mgx8850**

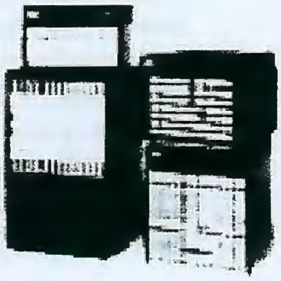
Cisco MGX 8830 ATM Multiservice Switch

The Cisco MGX 8830 Advanced ATM Multiservice Switch extends a full suite of narrowband interfaces and broadband trunking to remote sites with low density and high service mix requirements, using PNNI and MPLS for flexible network and services evolution. The Cisco MGX 8830, with a switching capacity of up to 1.2 Gbps, acts as a standalone switch, and offers a full range of service interfaces.

For More Information

See the Cisco MGX 8830 Series Web site: **http://www.cisco.com/go/mgx8830**

Cisco MGX 8200 Series



Cisco MGX 8230 Edge Concentrator

The Cisco MGX 8230 Edge Concentrator provides the most cost-effective gateway for narrowband services in space and power limited situations. It can acts as a stand-alone gateway or as an edge concentrator for the Cisco BPX 8600, Cisco MGX 8850 with PXM-45, and IGX 8400 series multiservice switches. The MGX 8230 offers a full range of narrowband service interfaces and a switching capacity up to 1.2 Gbps.

Cisco MGX 8250 Edge Concentrator

The Cisco MGX 8250 is a high-density edge concentrator designed for service providers needing flexibility for aggregation of IP, voice, Frame Relay, circuit emulation, and ATM services. An ATM narrowband edge concentrator, the MGX 8250 can serve as a stand-alone edge concentrator or as a feeder node for the Cisco BPX 8600 series and MGX 8850 switches. The MGX 8250 Edge Concentrator offers up to 1.2 Gbps of IP + ATM switching capacity.

For More Information

See the Cisco MGX 8200 Series Web site: **http://www.cisco.com/go/mgx8200**

Cisco IGX 8400 Series Multiservice WAN Switch

Efficient bandwidth utilization, intelligent QoS management features, and carrier-class reliability make the IGX 8400 series switch the ideal choice for meeting unique Wide-Area Networking (WAN) needs. This series provides the ATM backbone required to deliver data, voice, fax, and video services with guaranteed quality of service (QoS). The IGX 8400 series switch connects to public services for reduced leased-line costs by maximizing the use of these WAN links. Available with 8, 16, or 32 slots, the IGX 8400 series switches offers high flexibility to meet a wide range of Enterprise and Service Provider needs. Tight integration with the broad range of Cisco access products enables you to efficiently and cost-effectively run backbone-to-branch data, voice, fax, and video services between premises. By integrating IOS technology, the Cisco IGX 8400 series switch helps deliver a seamless migration path to technologies such as VoIP and MPLS.

For More Information

See the Cisco IGX 8400 Web site: **http://www.cisco.com/go/igx**

Cisco Long Reach Ethernet Solution

The Cisco Long-Reach Ethernet solution meets the demands of high bandwidth applications while leveraging existing copper wiring infrastructures. Catalyst® 2950 Long-Reach Ethernet (LRE) Series switches enable enterprise and service provider customers to extend intelligent Ethernet services over existing phone and legacy wiring, at distances of up to 5000 feet. Cisco is the only company with the breadth of technologies that allow customers to deliver intelligent network services across any combination of wired and wireless infrastructures.

The Cisco 2950 LRE solution includes the Cisco Catalyst® 2950 LRE switches, the Cisco 575 and 585 LRE Customer Premise Equipment (CPE) devices, and the Cisco LRE POTS Splitter. Each LRE link is terminated with either the Cisco 575 or 585 LRE CPEs, and a POTS splitter is required when POTS traffic coexists with the LRE link over the same line.

Catalyst 2950 LRE Series Intelligent Ethernet Switches

The Cisco Catalyst® 2950 LRE switches are fixed-configuration, stackable models that provide wire-speed LRE and Gigabit Ethernet connectivity for small and midsized networks. The Catalyst 2950 Series is an affordable product line that brings intelligent services, such as enhanced security, high availability and advanced quality of service (QoS), to the network edge-while maintaining the simplicity of traditional LAN switching. When a Catalyst 2950 LRE switch is combined with a Catalyst 3550 Series switch, the solution can enable IP routing from the edge to the core of the network. Embedded in Catalyst 2950 Series switches is the Cisco Cluster Management Suite (CMS) Software, which allows users to simultaneously configure and troubleshoot multiple Catalyst desktop switches using a standard Web browser. In addition to CMS, Cisco Catalyst 2950 LRE switches provide extensive management tools using Simple Network Management Protocol (SNMP) network management platforms such as CiscoWorks for Switched Internetworks.

The Cisco Catalyst 2950 LRE switches consist of the following devices-which are based upon the Enhanced Image (EI) Software for the Catalyst 2950 Series.

- Catalyst 2950ST-24-LRE-24 LRE ports + 2 10/100/1000BASE-T ports + 2 Small Form-Factor Pluggable (SFP) ports (two of the four uplinks active at one time)
- Catalyst 2950ST-8-LRE-8 LRE ports + 2 10/100/1000BASE-T ports + 2 SFP ports (two of the four uplinks active at one time)

The two built-in Gigabit Ethernet SFP ports support 1000BASE-SX and 1000BASE-LX modules. The dual SFP-based and copper Gigabit Ethernet implementation provides customers with tremendous deployment flexibility-allowing customers increased availability with the redundant uplinks. High levels of stack resiliency can also be implemented by deploying dual redundant Gigabit Ethernet uplinks and UplinkFast technologies for high-speed uplink and stack interconnection failover, and Per VLAN Spanning Tree Plus (PVST+) for uplink load balancing.

Cisco 575 and 585 LRE CPE Devices

Each LRE port is terminated in the room with either the Cisco 575 or 585 LRE Customer Premise Equipment (CPE) devices. These compact devices bridge LRE and Ethernet. The 575 CPE has one RJ-45 Ethernet connection and two RJ-11 connectors—one for the wall and one for a telephone. The 585 CPE has four RJ-45 switched Ethernet connections and two RJ-11 connectors and supports 802.1p QoS so that voice and video traffic are prioritized over normal data traffic. Both the Cisco 575 and 585 LRE CPE device can be mounted on or under a desk, or on a wall. They ship with a mount lock-in mechanism and clip-on Ethernet cable guard to discourage theft. It supports voice (Plain Old Telephone Service—POTS) traffic-including ISDN or digital phones-that coexists over the same LRE line by splitting LRE and POTS traffic at the CPE device.

Cisco LRE 48 POTS Splitter

The Cisco LRE 48 POTS Splitter is a high-density, low-cost device that is ideal for building deployments where the PBX system is on-site and POTS traffic must coexist over the same copper wiring as LRE traffic. Unlike "splitterless" building broadband network solutions, the Cisco LRE 48 POTS Splitter ships as a separate, compact form factor to ensure that POTS service is separate, and never compromised by LRE switch reconfigurations or downtime.

The Cisco LRE 48 POTS Splitter supports 48 ports in a 1RU form factor. Each splitter has six RJ-21 connectors-two each for connectivity to the patch panel, the LRE switch(es), and the on-site PBX system.

Key Features

- Performance—Delivers 2-15 Mbps symmetric over existing category 1/2/3 wiring at distances up to 5000 feet. Rate Selection feature automates the process of selecting a data rate for a line for ease of installation and increased robustness.
- Powerful Gigabit Ethernet uplink options—1000BaseT and SFP ports
- Superior control through intelligent services—advanced quality of service and security based on Layer 2 through Layer 4 parameters.
- Multicast support—Multicast VLAN Registration (MVR) and IGMP Snooping.
- Enhanced Cisco IOS Services
- Network Management—Cisco Switch Clustering technology and the advanced, Web-based Cisco Cluster Management Suite (CMS) software deliver easy-to-use configuration and ongoing monitoring and management of up to 16 switches. This software is embedded in the switches and delivers remote management of clustered switches and connected CPE devices through a single IP address

Competitive Products

• Paradyne Networks: BitStorm solution (Etherloop) and ReachDSL products	• Extreme Networks: Alpine chassis with FM-8Vi blade (Ethernet over VDSL)
• Tut Systems: IntelliPOP VDSL	• Huawei: Quidway s3026v

Specifications

Feature	Cisco 2950ST 24 LRE	Cisco 2950ST 8 LRE
Fixed Ports	24 Long-Reach Ethernet ports and four 10/100 Ethernet ports and 2 10/100/1000BASE-T ports + 2 Small Form-Factor Pluggable (SFP) ports (two of the four uplinks active at one time	12 Long-Reach Ethernet ports and four 10/100 Ethernet ports and 2 10/100/1000BASE-T ports + 2 Small Form-Factor Pluggable (SFP) ports (two of the four uplinks active at one time)
Backplane	8.8 Gbps	Same as Cisco 2950ST 24 LRE

7609
3

Feature	Cisco 2950ST 24 LRE	Cisco 2950ST 8 LRE
Forwarding Rate	3.5 Mpps	3.2 Mpps
VLAN Maximum	250 port based VLANs or ISL/802.1Q trunks	Same as Cisco 2950ST 24 LRE
FEC	Yes	Same as Cisco 2950ST 24 LRE
802.1Q	Yes	Same as Cisco 2950ST 24 LRE
Multicast	IGMP Snooping	Same as Cisco 2950ST 24 LRE
QoS	802.1 p, 4 egress queues, WRR, Layer 3 and 4 services	Same as Cisco 2950ST 24 LRE
Management Capabilities	SNMP, Telnet, RMON, CWSI, CLI-based out-of-band, embedded Cisco Cluster Management Suite (CMS), Web-based interface	Same as Cisco 2950ST 24 LRE
Memory	84 MB (Flash); 32 MB (CPU DRAM)	Same as Cisco 2950ST 24 LRE
Embedded RMON	History, Events, Alarms, Statistics	Same as Cisco 2950ST 24 LRE
Dimensions (HxWxD)	1.75" (44.5 mm) x 17.5" (444.5 mm) x 9.7" (246.6 mm)	Same as Cisco 2950ST 24 LRE

Selected Part Numbers and Ordering Information[1]

Catalyst 2950 LRE Series Switches	
WS-C2950ST-24-LRE	Catalyst 2950 LRE switch: 24-port LRE + 2 10/100/1000BASE-T ports + 2 SFP ports
WS-C2950ST-8-LRE	Catalyst 2950 LRE switch: 8-port LRE + 2 10/100/1000BASE-T ports + 2 SFP ports
Cisco 575 and 585LRE CPE Device	
CISCO575-LRE	Cisco 575 LRE CPE device: 1-port Ethernet + 2 RJ-11 connectors
CISCO575-LRE-6P	Cisco 575 LRE CPE device (6 pack): 1-port Ethernet + 2 RJ-11 connectors
CISCO575-LRE-24P	Cisco 575 LRE CPE device (24 pack): 1-port Ethernet + 2 RJ-11 connectors
CISCO585-LRE	Cisco 585 LRE CPE device: 4-port Ethernet + 2 RJ-11 connectors
CISCO585-LRE-6P	Cisco 585 LRE CPE device (6 pack): 4-port Ethernet + 2 RJ-11 connectors
CISCO585-LRE-24P	Cisco 585 LRE CPE device (24 pack): 4-port Ethernet + 2 RJ-11 connectors
Cisco LRE 48 POTS Splitter	
PS-1M-LRE-48	Cisco LRE 48 POTS Splitter: 48 ports

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the LRE Web site: **http://www.cisco.com/go/lre**

Cisco Building Broadband Service Manager (BBSM) Version 5.2

Cisco Building Broadband Service Manager (BBSM) is an access gateway for public access networks that enables simple, plug-and-play access, end user self-provisioning of services, customizable portal and advertising platforms and Web-based management, reporting and configuration. In addition, multiple automated authentication and billing options are supported, including credit card, RADIUS, property management system and access code.

The Cisco BBSM platform manages Internet access services with no routine IT support, enabling property owners and service providers to offer services in remote and unattended locations. BBSM supports tiered service levels in order to deliver targeted customer offerings. For instance, a hotel can set-up daily network access for a series of meetings providing a variety of bandwidth/pricing options to capture lucrative meeting room revenue opportunities.

The Cisco BBSM has been designed for compatibility with Cisco access-layer LAN products to provide a complete solution that enables service providers or property owners to create, market and operate broadband access services in new vertical markets such as: Hospitality, Higher-Education, and Public Access

Cisco BBSM Hotspot Server Version 1.0

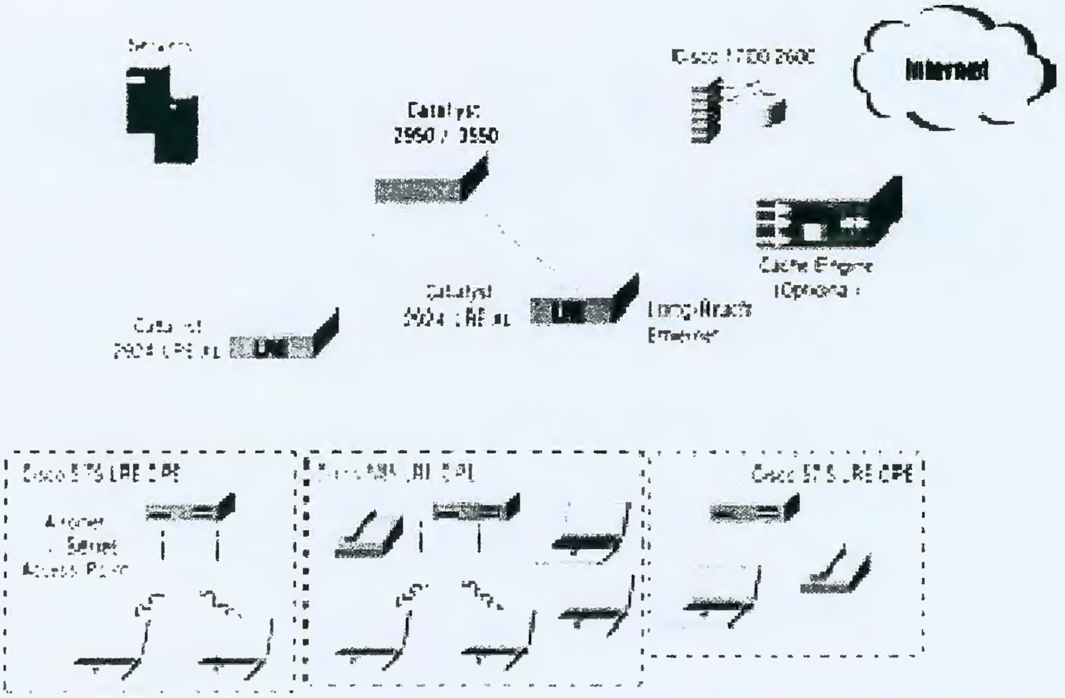
The Cisco Building Broadband Service Manager (BBSM) Hotspot server connects mobile users to broadband services anywhere, anytime. Cisco BBSM Hotspot is a cost effective access management gateway suited for small- to medium-sized public access locations, as well as for visitor access in larger enterprise locations. BBSM Hotspot enables simple plug-and-play connectivity, end user self-provisioning of services, and multiple authentication options.

BBSM Hotspot works with Cisco Local Area Network (LAN) products to provide a complete solution for secure wired and wireless Internet Access for visitors, guests and other temporary users. Use Cisco BBSM Hotspot to manage and operate broadband access services in public hotspots, small hotels, and public overlays on business networks.

For More Information

See the BBSM Web site: **http://www.cisco.com/go/bbsm**

Sample LRE Solution Overview—Broadband Internet Access for MxU



CHAPTER 8

Optical Transport

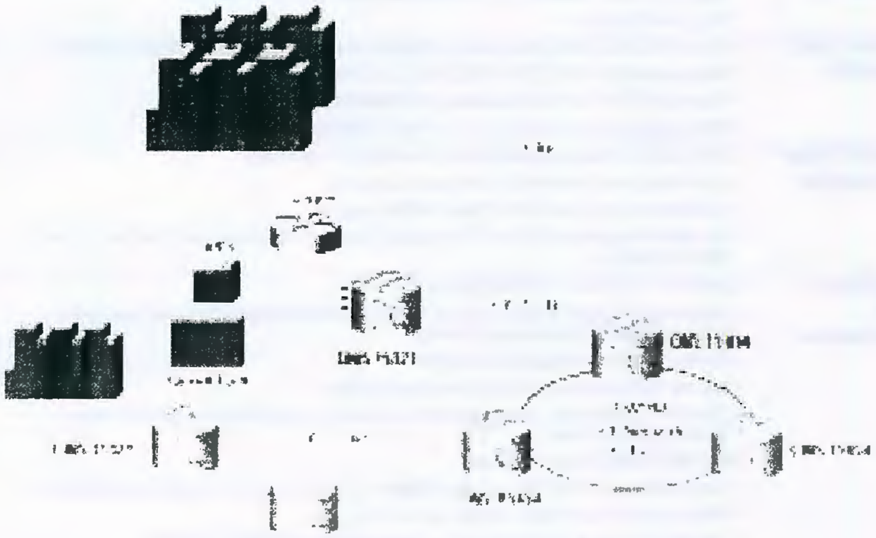
Optical Transport Products at a Glance

Product	Features	Page
Cisco ONS 15200 Metro DWDM Series	Cisco ONS 15252 and ONS 15201 DWDM solutions • Supports a mixture of point-to-point, hubbed, and meshed traffic patterns (SDH/SONET, Gigabit Ethernet over a range of line rates up to 2.5 Gbit/s) • Modular architecture, capacity may be added channel-by-channel in a highly cost-effective manner • High transmission efficiency for more channels, nodes and greater distances • Compact design	8-3
Cisco ONS 15302/15305 SDH Multiservice CPE & Aggregation Platforms	The Cisco ONS 15302/ONS 15305 Multiservice CPE and aggregation solutions are ultra-compact integrated systems that extend next-generation optical networks (access nodes or CPE): • Low Cost Access or CPE Platform • E1, E3, DS3, 10/100 BaseT Ethernet and GigE • STM-1 (15302) or STM-1/4/16 (15305)	8-3
Cisco ONS 15327 SONET Multiservice CPE & Aggregation Platform	Metro Edge Multiservice Provisioning Platform (MSPP) • Highly cost-efficient for delivering multiservices to the metro edge • Aggregates and switches TDM, 10/100/GigE, data and video services • Very small footprint	8-4
Cisco ONS 15454 SONET and ONS 15454 SDH Platforms	Industry-leading SONET Multi-service Provisioning Platform (MSPP) and SDH MSPP: • Aggregates DS1, DS3, STS-1, OC-3, OC-12, OC-48 • Supports OC-192 and mulitwavelength DWDM optics • Wide range of data interfaces, including 10/100/GigE, data and video	8-4
Cisco ONS 15501 Erbium Doped Fiber Amplifier	• Designed for Enterprise and Service Provider environments • Low-noise, gain flattened C-band optical amplifier • Complements the Cisco ONS 155xx DWDM solution • Capable of extending 100GHz, 32-channel, 2.5Gbps / 10Gbps optical infrastructure over longer distances	8-5
Cisco ONS 15216 and 15501 Optical Transmission Families	Cisco ONS 15216 Metro DWDM Series • Supports 32 ITU-grid wavelengths at 100 GHz spacing and provides unprecedented transport flexibility with optical filtering • Optical Add/Drop Multiplexing (OADM) • Optical Performance Monitoring and Amplification • The ONS 15216 allows carriers to deliver more services per wavelength and more wavelengths per fiber Cisco ONS 15501 Optical Amplifier • Constant flat gain of 17 dB over the 1530nm to 1563nm band simplifies network design. • Metro optimized auto gain control and variable gain • Low noise figure of <6.0 dB allows the use multiple amplifiers in cascade • Input power range of -29 to 0 dBm	8-5
Cisco ONS 15530 Metro DWDM Aggregation Platform	Metro Optical DWDM Multiservice Aggregation Platform • Enables storage and data networking, transparent wavelength services, and legacy applications • ESCON Aggregation up to 40 channels on 1 wavelength • Scales from 2.5Gbps to 10Gbps • Supports wide range of protocols over optical infrastructure • Highly resilient network with flexible topology design options	8-5

7605 G

Product	Features	Page
Cisco ONS 15540 Extended Services Platform	Highly modular and scalable next-generation Dense Wave Division Multiplexing (DWDM) platform • Ideal for enterprises and service providers • Delivers the integration of data, storage and metro networking • Ultra-high bandwidth intelligent optical infrastructure • Supports any packet on any wavelength from any platform	8-6
Cisco ONS 15600 Multiservice Switching Platform (SONET/SDH)	The Cisco ONS 15600 MSSP is a true multiservice switch, providing carrier class reliability, availability, serviceability, operations, and management. • Combines the functionality of multiple metro systems including SONET/SDH multiplexers and digital cross-connect network elements • Scalable, easy-to-use platform supports all metrotopologies	8-7
Cisco Transport Manager (CTM 4.x) (Network Management)	Carrier-class element management system • Ideal for service provider and enterprise networks • Supports Cisco ONS 15454/15327/15600 (SONET/SDH), 15540, 15530, 15501, 152xx, 1580Xsystems • Manages fault /performance/configuration/alarm/security/inventory/administrative tasks • Native Circuit/Equipment Provisioning for 15454/15327/15600 SONET/SDH product family • Northbound interfaces include SNMP, TL1 and CORBA • Integrates into OSS/BSS systems • Requires SUN/Solaris/UNIX server and Oracle database	8-8
Cisco 10720 Internet Router	Service provider-class metro access services router • Optimized building block for the next generation metro IP network • Equipped with 24 ports of Ethernet technology for customer access and dynamic packet transport (DPT) technology for metro optical connectivity • Powered by Cisco IOS software and the parallel express forwarding (PXF) architecture • Cost-effective, reliable platform supporting full suite of IP routing protocols • With DPT architecture, enables optimal fiber connectivity as well as features such as IP class of service, TLS, VoIP and VPN services See Chapter 1—Routers for more information on the Cisco 10720 Internet Router	1-49

Sample Metro Optical Transport Solution Overview—Delivering Multiservices to the Edge



Cisco ONS 15200 Optical Metro DWDM Series

The Cisco ONS 15252, 15201, and 15216 are part of the Cisco ONS 15200 Metro DWDM family, the first solution to deliver instant wavelengths to buildings, premises, or PoPs.

The ONS 15252 and 15201 may be used to realize many sub-network topologies and can handle a mixture of point-to-point, hubbed, and meshed traffic patterns. Capacity may be added channel-by-channel in a highly cost-effective manner. Since they feature broadband transponders, a wide range of traffic types may be handled (SONET/SDH, Gigabit Ethernet) over a range of line rates up to 2.5 Gbs. Channel protection options include unprotected, client-protected, and (optical channel) fiber protection. The ONS 15252 is a multi-channel unit and the ONS 15201 is a single channel unit node. Both have exceptionally small footprints and low power consumption.

The Cisco ONS 15216 supercharges wavelength services by supporting up to 32 ITU-grid wavelengths, and provides unprecedented transport flexibility with optical filtering, Optical Add/Drop Multiplexing (OADM), Optical Performance Monitoring and Amplification. It allows service providers to deliver more services per wavelength and more wavelengths per fiber.

The Cisco ONS 15216 optical filter solution enables service providers to deploy point-to-point, bus, and ring networks using the terminal filter multiplexing and demultiplexing and OADM. The Cisco ONS 15216 platform provides an open and flexible solution to combine wavelengths launched by the Cisco ONS 15454, ONS 15252, ONS 15201, and ONS 15540. The Cisco ONS 15216 supercharges wavelength services and extends Cisco's optical leadership to metro regional DWDM.

For More Information

See the ONS 15200 Series Web site: **http://www.cisco.com/go/ons15200**

Cisco ONS 15302/15305 SDH Multiservice CPE & Aggregation Platforms

The Cisco ONS 15302/ONS 15305 Multiservice CPE and Aggregation solutions are ultra-compact integrated systems that offer cost effective solutions with short ROI. These platforms provide native multiservice capabilities (i.e., TDM interfaces, multiplexing and Ethernet data interfaces). These products can be managed under Cisco Transport Manager (CTM), Cisco's unified optical network management system.

The ONS 15302 CPE platform provides the following TDM interfaces—STM-1 uplink (protected or unprotected STM-1 optical uplink, 1+1 MSP, future SNCP) and E1 customer interfaces (12 E1 ports). This product also provides native Ethernet customer access via 4-port 10/100BaseT module that supports full layer 2 capacity, bridging, VLANs, spanning tree, and priority management. An optional WAN module is available for point to multi-point applications.

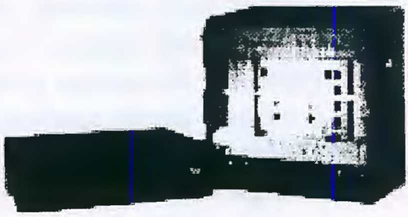
The ONS 15305 Aggregation platform provides the following TDM interfaces—protected or unprotected optical interfaces (8 port S-1.1 optical module, 2 port S-4.1 optical module, 1 port S-16.1 optical module, 1+1 MSP, SNCP, 2F MS-SPRing for STM-16) and electrical customer interfaces (8 and 63 port E1 modules and a 6 port

E3/DS3 module). This product also provides native Ethernet customer access via an 8-port 10/100BaseT module and a 2-port GigE module (supports full layer 2 capacity, bridging, VLANs, spanning tree, and priority management). An optional WAN module is available for point to multi-point applications.

For More Information

See the ONS 15302/ONS 15305 web site: **http://www.cisco.com/go/ons15300**

Cisco ONS 15454 and 15327 Multiservice Provisioning Platforms



The Cisco ONS 15454 and ONS 15327 Multi-service Provisioning Platforms (MSPP) are key building blocks in today's optical networks due to their unprecedented transport performance and economics. They offer supercharged transport capability by combining the best of traditional SONET TDM (time division multiplexing) and statistical multiplexing in single units.

The Cisco ONS 15454 aggregates traditional facilities such as DS1, DS3, STS-1, OC-3, OC-12, and OC-48 including multi-wavelength DWDM optics, but it also supports data interfaces for 10/100/GigE, data and video. This enables drastically improved efficiencies in the transport layer and breakthrough cost savings for initial and life cycle deployment. A single ONS 15454 shelf can support combinations of OC-3/c, OC-12/c, OC-48/c, and OC-192.

The new Cisco ONS 15454 SDH MSPP offers an international optical transport solution that combines the best of traditional SDH TDM and statistical multiplexing in a single platform. The Cisco ONS 15454 SDH MSP can aggregate traditional services such as E1, E3, DS3, STM-1, STM-4, STM-16 and STM-64 including multi-wavelength DWDM optics, but is also designed to support data interfaces such as Ethernet/IP.

The Cisco ONS 15327 combines industry-leading bandwidth capacity and service diversity in a very compact footprint, enabling service providers to achieve radical economics at the metro edge. Based on the same technology as the industry leading Cisco ONS 15454, the ONS 15327 supports high optical bandwidth and has the ability to drop a DS1 from an OC-48 stream. With comprehensive STS- and VT-level bandwidth management and integrated data switching, the Cisco ONS 15327 also serves as a digital cross-connect without the need for additional equipment. It aggregates and switches TDM, Ethernet, and ATM services, and can be managed using the Cisco Transport Manager element management system.

For More Information

See the ONS 15454 SONET Web site: **http://www.cisco.com/go/ons15454**

See the ONS 15454 SDH Web site: **http://www.cisco.com/go/15454sdh**

See the ONS 15327 Web site: **http://www.cisco.com/go/ons15327**

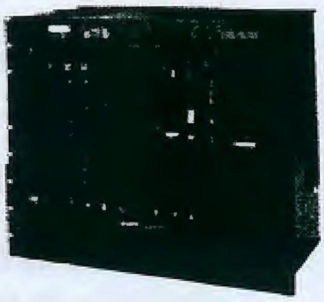
Cisco ONS 15501 Erbium Doped Fiber Amplifier

The Cisco ONS 15501 is a low-noise, gain-flattened C-band optical erbium doped fiber amplifier designed to extend the distance of today's metro high-bandwidth optical network beyond existing optical budget constraints. The Cisco ONS 15501 complements the Cisco ONS 155xx DWDM and Catalyst 6500 solutions, providing customers with the capability to extend their 2.5-Gbps or 10-Gbps optical infrastructures over greater distances. Packaged in a one-rack-unit (1RU) chassis, the Cisco ONS 15501 incorporates features such as 17-dB constant flat gain, automatic gain control, and low noise figure for excellent Optical Signal to Noise Ratio (OSNR) characteristics.

For More Information

See the Cisco ONS 15501 Web site: **http://www.cisco.com/go/ons15501**

Cisco ONS 15530



The Cisco ONS 15530 is a DWDM (dense wavelength division multiplexing) multiservice aggregation platform. The ONS 15530 can be used in applications such as storage networking, data networking, transparent wavelength services, and legacy SONET / SDH / ATM. These features make the ONS 15530 an excellent choice for building a scalable, ultra-high-bandwidth-ready, intelligent optical aggregation and transport infrastructure.

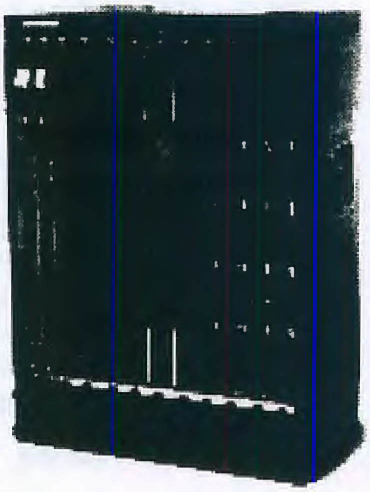
Key Features

- Aggregation—up to 40 ports of ESCON or 8 ports of Fibre Channel, FICON, or Gigabit Ethernet per wavelength, lowering total cost of ownership through bandwidth efficiency
- Scalability—up to 32 wavelengths ranging from 2.5Gbps to 10Gbps for network growth and design flexibility
- Multiservice Interfaces—protocol-independent transponders supporting data rates between 16Mbps to 2.5Gbps for protocols such as ESCON, FICON, Fibre Channel, 2G Fibre Channel, Gigabit Ethernet, SONET/SDH, Digital Video, and other protocols
- Cost-efficient point-to-point fiber trunk protection capability using the Protection Switch Module
- Complete Amplification Solution—Together with ONS 15501 EDFA optical amplifier, the VOA modules enables enterprises and service providers to further expand their optical DWDM networks over greater distances.
- Design Flexibility—can be used to deploy Point-to-point, Hub Ring, or Mesh Ring networks
- Network assurance—through high availability and resilient optical design
- IOS-based—easily integrates into existing Cisco networks

For More Information

See the Cisco ONS 15530 Web site: **http://www.cisco.com/go/ons15530**

Cisco ONS 15540 Extended Services Platform (ESPx)



The ONS 15540 Extended Services Platform with external cross connect capability (ESPx) is a highly modular, flexible, and scalable next generation dense wave division multiplexer (DWDM) platform that integrates data networking, storage area networking (SAN), time division multiplexing, (TDM) Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) technologies over an ultra high bandwidth, intelligent optical infrastructure that can support any packet, over any wavelength on any platform.

- Flexible Multi-Protocol Support—The Cisco ONS 15540 offers both variable rate transparent and fixed rate multi-protocol transponders that feature user selectable small form factor pluggables (SFPs) and support a variety of industry standard data rates between 16Mbps to 2.5Gbps as well as 10Gb Ethernet
- Scalable, flexible, and modular architecture in a high-density compact footprint—Provides superior operational support and network expansion on an as needed basis through its hot swappable modular lines cards, transponders, and optical multiplexers
- Simple Network Consolidation and Comprehensive Multi Service Support provided by the available ONS 15540 2.5GB and 10GbE transponders
- Optical, Service, and Application Level Performance Monitoring—provides industry-leading supports for service level agreements (SLAs)
- High Availability for mission critical networks—Provides 99.999% availability for demanding Managed Network Service Providers and enterprise business continuance applications, with hardware redundancy and automatic protection switching to protect against fiber cuts and equipment failures
- Multi-Service Integration—Transports ESCON, FICON, 1Gb/2GB Fibre Channel for Storage Area Networking (SAN), Fast and Gigabit Ethernet, and 10 Gb Ethernet for data networking, and SONET/SDH at OC-3/STM1, OC-12/STM4, and OC-48/STM12

Key Features:

- Compact modular design with external connectorization: External Direct Connect system from Line card to OADMs; Optional cross connect and fiber management system
- Transparent Tuneable Variable data rate Type 1 Transponders: 16Mbps to 622Mbps MM fiber support; 16Mbps to 2.5Gbp SM fiber support; 16 Tuneable transponders support 32 channels for reduced sparing costs; Multi-protocol support for Enterprise
- Tuneable Type 2 Transponders with Multi Protocol Small form Factor Pluggables (SFPs): Variable data rate support between 16Mbps to 2.5Gbps; 16 Tuneable transponders support 32 channels for reduced sparing costs; Multi-protocol SFP Support
- Standards based Management support for SNMP, Ciscoview and Cisco Transport Manager (CTM)
- Protection Switch Module provides highly cost effective solution for fiber trunk protection
- Standards based Optical architecture conforming to ITU G.692 100GHz channel spacing
- This system has been qualified by IBM for Geographically Dispersed Parallel Sysplex (GDPS), and by EMC for Symmetrix Synchronous support as tested in their E-LAB environment

For More Information

See the Cisco ONS 15500 Series Web site: **http://www.cisco.com/go/ons15500**

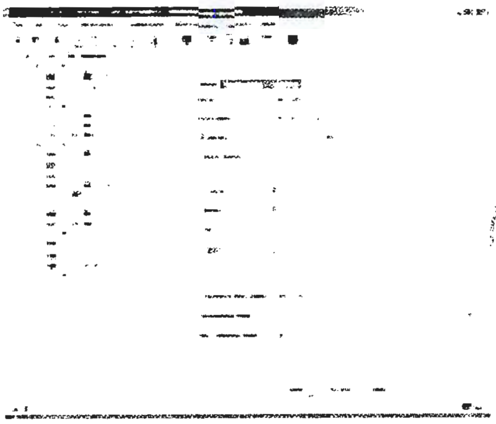
Cisco ONS 15600 Multiservice Switching Platform

The Cisco ONS 15600 provides unparalleled flexibility in designing next generation metro networks. Fully engineered and optimized for metro networks, the Cisco ONS 15600 MSSP simplifies and revolutionizes bandwidth management in the metro core by allowing service providers to seamlessly integrate their metro core and metro edge networks, while dramatically reducing initial turn up costs. Delivering scalability to 960 Gbps of traffic in a single rack, it complements the market-leading Cisco ONS 15454 Multiservice Provisioning Platform (MSPP) by leveraging its proven architecture and operating software. This allows service providers to dramatically simplify their metro networks and realize immediate cost, space and operational benefits. The Cisco ONS 15600 MSSP provides complete integration of metro core and edgenetworks for service provisioning and network management.

For More Information

See the ONS 15600 Series web site: **http://www.cisco.com/go/ons15600**

Cisco Transport Manager (CTM 4.x) (Element/Network Management)



Cisco Transport Manager is an integrated optical element management system for Cisco ONS 15000 series optical networking platforms. CTM manages configuration, fault isolation, performance, and security for Cisco optical network elements. With integrated support for SONET, SDH, DWDM and Ethernet, along with open interfaces to operations support systems (OSS), CTM delivers the full power of Cisco's wide range of advanced optical systems to today's network operators and enterprises.

7599
E

CHAPTER 9

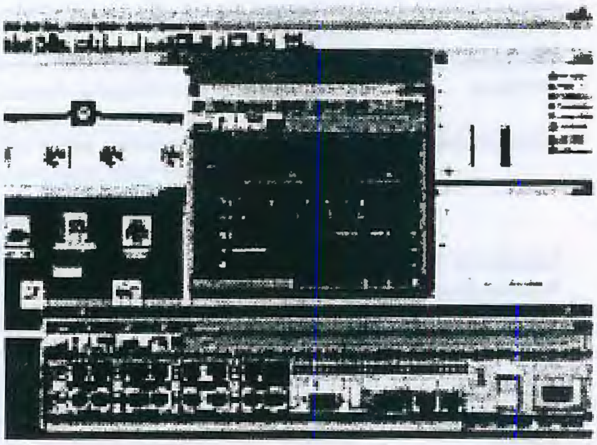
IOS Software & Network Management

Cisco IOS® Software & Network Management Products at a Glance

Product	Features	Page
CiscoWorks for Windows	An entry level suite of integrated network management tools for smaller networks: • Event management and topology mapping application • Includes Cisco's popular CiscoView Element Management Tool	9-2
Cisco IOS Software	Feature-rich network operating system supported on wide range of Cisco products • Provides a common IP fabric, functionality, and command-line interface (CLI) across network infrastructures • Enables a vast array of key routing, multiservice, traffic shaping, security/firewall, and traffic monitoring applications, and a broad variety of network connections	9-4
CiscoWorks Small Network Management Solution	Web-based network management solution designed for small to medium businesses (SMB) • Device auto-discovery using SNMP simplifies setup and reduces startup time • Standards-based, multi-vendor management • Event management and topology mapping application • Includes Cisco's popular CiscoView Element Management Tool	9-11
CiscoWorks Routed WAN Management Solution	A comprehensive set of applications for managing the router elements of a multiservice Enterprise wide-area network. This bundle includes Access Control List Manager, Internetwork Performance Monitor, Resource Manager Essentials, and CiscoView	9-13
CiscoWorks LAN Management Solution	Provides key applications needed to manage Cisco switch-based Enterprise campus networks. This bundle includes Campus Manager, Device Fault Manager, nGenius Real Time Monitor, Resource Manager Essentials, and CiscoView	9-14
CiscoWorks VPN/Security Management Solution	Combines general device management tools for configuring, monitoring, and troubleshooting enterprise networks with powerful security solutions for managing virtual private networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS). This bundle includes Management and Monitoring Centers, Cisco IDS Host Sensor and Console, Cisco Secure Policy Manager, VPN Monitor, Resource Manager Essentials, and Cisco View	9-16
CiscoWorks Manager IP Telephony Environment Monitor	A suite of telephony management applications that ensures the readiness and manageability of converged networks supporting VoIP and IP telephony traffic and applications. The bundle includes Voice Health Monitor, Default Fault Manager, CiscoView, and Downloadable Modules: IP Phone Information Utility, IP Phone Help Desk Utility, Fault History Manager	9-18
CiscoWorks Voice Manager for Voice Gateways	Enables the management and monitoring of devices used as gateways between analog voice equipment and the data network. • Enhanced capabilities to configure and provision voice ports • Create and modify dial plans on voice-enabled Cisco routers for voice over IP (VoIP), voice over Frame Relay (VoFR), and voice over ATM (VoATM) network deployments	9-19
CiscoWorks QoS Policy Manager (QPM)	Enables centralized administration and automated deployment of bandwidth reservation and prioritization policies for critical network applications • Differentiates services of Web applications, voice traffic, and business-critical applications	9-21
Cisco Ethernet Subscriber Solution Engine	A hardware-based management system for metro access networks that use the Cisco ONT 1000 Gigabit Ethernet Series Optical Network Terminator. • Enables complete remote management and troubleshooting of the customer demarcation point for Ethernet over fiber	9-22
CiscoWorks Hosting Solution Engine	A hardware-based content management solution for e-business operations in Cisco-powered data Centers. This product provides network infrastructure monitoring and Layer 4-7 hosted services configuration and activation.	9-24
CiscoWorks Wireless LAN Solution Engine	A hardware paced wireless LAN management solution that provides template-based configuration with user-defined groups to effectively manage a large number of access points and bridges • Monitors LEAP authentication servers • Enhances security management through mis-configuration detection on access points and bridges	9-23
Cisco Catalyst 6500 Series Network Analysis Modules 1 and 2	NAM is an integrated, network monitoring instrumentation and Web-browser based traffic analysis solution for the Catalyst 6500 based environments. It enable greater visibility into traffic at all layers of the network by providing real time traffic analysis and troubleshooting capabilities.	9-25

Product	Features	Page
Cisco Secure User Registration Tool (URT)	Provides organizations with increased LAN security by actively identifies users within the network and creates user registration policy bindings that help support mobility and tracking: • Ensures that users are associated with their authorized subnet/VLAN; Addresses the challenges associated with campus user mobility; Supports Web-based authentication for Windows, Macintosh, and Linux client platforms; Secure user access to the VLAN with MAC address-based security option Option to allow multiple users connected to a hub access to a VLAN served by single switch port See Chapter 5—VPN and Security for more information on Cisco Secure User Registration Tool	5-15
Cisco Secure Access Control Server (ACS) for Windows	Controls the authentication, authorization, and accounting (AAA) of users and administrators to network devices and services; Operates as a centralized Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+) server; Supports Lightweight Directory Access Protocol (LDAP) user authentication; Data replication and backup services; Flexible user and group policy controls; Support for Cisco 802.11x Catalyst Switch and Wireless solutions; Extensible Authentication Protocol (EAP) enhancements to support Protected EAP (PEAP) for wireless LANs All administrative access is encrypted with SSL See Chapter 5—VPN and Security for more information on CiscoSecure Access Control Server (ACS) for Windows	5-14

CiscoWorks for Windows



CiscoWorks for Windows is a powerful set of network management tools to easily manage your small to medium network or workgroup. It provides information such as dynamic status, statistics, and comprehensive configuration information for Cisco routers, switches, hubs, and access servers. Using the included WhatsUp Gold from Ipswitch, you can also monitor printer, workstations, servers and important non Cisco network services.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks for Windows	• A single solution for managing all resources attached to a small multivendor network • A smaller solution, where centralize management of configurations of a software distribution is not needed • Low-cost network management • Needs to quickly understand basic network connectivity, access individual device configurations and statistics, and troubleshoot problems

Also available for small and medium size customers is the CiscoWorks Small Network Management Solution (Small NMS). Small SNMS includes all the features above and includes CiscoWorks Resource Manager Essentials (Essentials) which provides additional functionality that allows the customer to of build and maintain an up-to-date hardware and software inventory for up to 20 devices in a network.

Key Features

CiscoWorks for Windows provides the following features when used in conjunction with WhatsUp Gold from Ipswitch (included in the CiscoWorks for Windows package):

- Automatic discovery process for networked devices
- Management of network hardware, printers, servers, and workstations
- Customizable monitoring of services such as FTP and HTTP
- Access to extensive data on port status, bandwidth utilization, traffic statistics, protocol information, and other network performance statistics
- Flexible graphing capabilities for quickly recording and analyzing historical data that can be exported to files
- Management Information Base (MIB) compiler and browser for managing third-party SNMP devices
- Tools to simplify device configuration and management for Cisco routers, switches, and access servers
- Threshold management features that can be set for many performance variables to generate an alarm or event notification
- Flexible event notification, including voice, paging, and e-mail notification of user-defined events

CiscoWorks for Windows Components

CiscoWorks for Windows includes the following tools:

- WhatsUp Gold from Ipswitch, Inc.—Provides network discovery, mapping, monitoring, and alarm tracking
- CiscoView—Provides back- and front-panel displays; dynamic, color-coded graphical displays simplify device-status monitoring, device-specific component diagnostics, and application launching
- Threshold Manager—Enhances the ability to set thresholds on Cisco RMON-enabled devices, reducing management overhead and improving troubleshooting capabilities
- StackMaker—Allows users to combine multiple Cisco devices of specific types into a single stack and visually manage them in a single window
- Show Commands—Displays detailed router system and protocol information without requiring the user to remember complex Cisco IOS Software command-line languages or syntax

Specifications

Feature	CiscoWorks for Windows
Hardware Requirements	266 MHz Pentium-based IBM PC or compatible computer 128-MB RAM total 1 GB free hard drive space
Software Requirements	Windows 98, Windows NT 4.0, or Windows 2000 Netscape 4.61, 4.7, 4.76 or Internet Explorer 5.0, 5.1, 5.5

Selected Part Numbers and Ordering Information

CiscoWorks for Windows	
CWW-6.1-WIN	CiscoWorks for Windows 6.1
CWW-6.1-WIN-UP	Upgrade to CWW 6.1 for Windows from CWW 5.0
CWW-6.1-WIN-MR	Maintenance Release: Requires existing CWW 6.0 -June 02

For More Information

See the CiscoWorks for Windows Web site: **http://www.cisco.com/go/cwwin**

Cisco IOS® Software

Cisco's IOS Software is a feature-rich network operating system that provides network intelligence for the majority of today's Internet and for most of the world's business-critical networking applications.

Supporting Cisco's extensive range of platforms, Cisco IOS Software provides a common IP fabric, functionality and command-line interface (CLI) across network infrastructures. Cisco IOS Software enables a vast array of key routing functions, multi-service capabilities, traffic shaping, connections, security/firewall protection, traffic monitoring, and highly flexible network and product configuration.

Below is an abbreviated list of key capabilities, intelligent network technologies, and architectures enabled by Cisco IOS Software:

- Quality of Service (QoS)
- Converged data, voice, and video over IP
- IP/ATM/Frame Relay network connectivity and scalability features
- Security/firewall/IPSec/access lists
- Traffic monitoring and NetFlow based monitoring, accounting, and billing
- Wide range of routing protocols (including MPLS)
- IPv6
- Multicast

Quality of Service (QoS)

The promise of networking is sharing networked resources among many users and applications for greater productivity and competitive advantage. Cisco IOS quality of services (QoS) capabilities enable complex networks to control and predictably service a variety of applications. Every network needs QoS for optimum efficiency, whether it is for a small business, large enterprise, or a service provider.

QoS expedites the handling of mission-critical applications, while sharing network resources with non-critical applications. QoS also ensures available bandwidth and minimum delays required by time-sensitive multimedia and voice applications. It also gives network managers control over network applications, improves cost-efficiency of WAN connections, and enables advanced differentiated services. QoS technologies are elemental building blocks for other Cisco IOS enabling services—particularly for converged data and voice networks (LAN/WAN + telephony), video conferencing over IP, and IBM networking, and for future business applications in campus, WAN, and service provider networks.

Key QoS Capabilities:

Committed Access Rate (CAR)	Performs two QoS functions: • Bandwidth management through rate limiting, which allows you to control the maximum rate for traffic sent or received on an interface • Packet classification through IP precedence and QoS group setting, which allows you to partition your network into multiple priority levels or classes of service (CoS)
Differentiated Services (DiffServ)	QoS architecture that divides traffic into a small number of classes and provides QoS to large aggregates of traffic by treating some traffic better than the rest (faster handling, more bandwidth on average, lower loss rate on average). This is a statistical preference, not a hard and fast guarantee.
Expedited Forwarding (EF)	Per-Hop Behavior (PHB) in the DiffServ standard, used to create a virtual leased line service.

Integrated Services (IntServ)	A QoS architecture in which each network element is required to identify the coordinated set of QoS control capabilities it provides in terms of the functions it performs, the information it requires, and the information it exports.
Random Early Detection (RED)	Monitors traffic levels on very large networks to prevent congestion and guarantee priority traffic delivery.
Resource Reservation Protocol (RSVP)	A protocol that supports the reservation of resources across an IP network.
Weighted Fair Queueing (WFQ)	Adds new levels of control to previous queuing methods
Weighted Random Early Detection (WRED)	Combines the capabilities of the random early detection (RED) algorithm with IP precedence or the differentiated services code point (DSCP). This combination provides for preferential traffic handling for higher-priority packets.

Key QoS Categories

Classification	• Committed Access Rate (CAR) • Policy Based Routing (PBR) • QoS Policy Propagation Through BGP
Congestion Management	• First in First Out (FIFO) • Priority Queueing (PQ) • Custom Queueing (CQ) • Weighted Fair Queueing (WFQ) • Weighted Random Early Detection (WRED)
Policy and Shaping	• Committed Access Rate (CAR) • Generic Traffic Shaping (GTS) • Frame Relay Traffic Shaping (FRTS)
Link Efficiency Mechanisms	• Compressed Real Time Protocol (CRTP) • Link Fragmentation and Interleaving (LFI) • Data Compression

Converged LAN/WAN and Telephony Networks

A broad range of Cisco products support standards-based voice over packet implementations, including H.323-based Voice over IP (VoIP). These products enable highly efficient, converged IP-based telephony in today's enterprise and service provider networks, thereby eliminating the need for legacy telephone equipment and overlay networks (including PBXs and central office circuit switched network equipment). Furthermore, a single IT organization can now support campus and enterprise requirements—regardless if for data, voice, or video requirements.

In addition, Cisco voice over packet technologies enable businesses and service providers to avoid long distance telephone charges by leveraging their existing data networks, instead of paying for dedicated voice connections and circuits.

Cisco Connectivity and Scalability Solutions

A wide range of access solutions are enabled via Cisco IOS Software including:

- Virtual Private Networking; DSL; Dial Access (including ISDN, modem, fax, voice)
- Frame Relay, X.25
- ATM; VoIP, VoFR, VoATM
- SONET, OC-x/STM-x, Packet-over-SONET
- Broadband Services Aggregation (includes large-scale PPPoE, PPPoA, L2TP tunneling)
- Cable Access Solutions

Security

Cisco's powerful suite of Cisco IOS Software-embedded security and firewall technologies includes:

Digital Signature Standard (DSS) and digital certification	Positively authenticates users or devices
Network Address Translation (NAT) and Port Address Translation (PAT)	Hides private topology and IP addresses from an external network
IPSec	Enables secure communications of data over public networks

Time-based Access Control Lists (ACLs)	Implements access lists based on time of day
Password Authentication Protocol (PAP)	Allows a remote node to establish its identity using a two-way handshake
Terminal Access Controller Access Control System Plus (TACACS+) and Remote Access Dial-in User Service (RADIUS)	Gives complete network access security for dial-in connections, for enterprise and service provider applications
Challenge Handshake Authentication Protocol (CHAP)	Allows a remote node to establish its identity using a three-way handshake
Calling Line Identification (CLID)	Uses calling line identification to compare the telephone number of a calling device against a list of known callers
Access Lists	Checks the source address of packets (standard access lists) and checks the source and destination addresses and other parameters (extended access lists)
Context-Based Access Control (CBAC)	Provides secure, application-based stateful filtering for the most popular protocols and a wide variety of advanced applications; available in the Cisco IOS Firewall feature set

Cisco IOS NetFlow

NetFlow technology provides the metering base for a key set of applications including network traffic accounting, usage-based network billing, network planning, network monitoring, outbound marketing, and data mining capabilities for both service provider and enterprise customers. Cisco provides a set of NetFlow applications to collect exported NetFlow data, to perform data volume reduction, and to post-process and display data. Cisco is currently working with a number of partners to provide customers with comprehensive solutions for NetFlow-based billing, planning, and monitoring. NetFlow also provides the measurement base for Cisco's new Internet Quality of Service (QoS) initiatives. NetFlow captures the traffic classification or precedence associated with each flow, enabling differentiated charging based on Quality of Service.

Furthermore, the combination of NetFlow data along with Cisco IOS Software-based routing information can prove key to developing effective security policies and preventive measures for Denial of Service (DoS).

Cisco IOS Routing Services

Cisco IOS Software has long been recognized for its rich support of multiple protocols including IP, Novell IPX, SNA, AppleTalk, DECnet, OSI, and Banyan VINES

IP Routing Protocols

Cisco IOS Software offers the industry's widest variety of enterprise and service provider-class routing protocols, including On Demand Routing (ODR), Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), IP Multicast, Integrated IS-IS, Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), and MPLS

Multi Protocol Label Switching (MPLS)

Cisco IOS MPLS fuses intelligent routing capabilities with the performance of switching. It provides significant benefits to networks with pure IP architectures and those with IP and ATM or a mix of other Layer 2 technologies. MPLS technology is key to implementing scalable Virtual Private Networks (VPNs) and end-to-end QoS, enabling efficient utilization of existing networks to meet growth needs and to rapidly correct link fault and node failure. This technology also helps deliver highly scalable, differentiated IP services with simpler configuration, management, and provisioning for both Internet service providers and end-user customers.

Common MPLS Applications Available with Cisco IOS Software

- Traffic engineering is enabled through MPLS mechanisms that allow traffic to be directed through a specific path, which may not necessarily be the least-expensive path. Network managers can implement policies to ensure optimal traffic distribution and improve overall network utilization
- Guaranteed bandwidth is a value-added enhancement to traditional traffic-engineering mechanisms. MPLS lets service providers deliver guaranteed pipes and bandwidth allocations. Guaranteed bandwidth also allows bookkeeping of quality-of-service (QoS) resources to traffic engineer both premium and best-effort traffic such as voice and data
- Fast reroute (FRR) allows extremely quick recovery if a node or link fails. Such fast recovery prevents end-user applications from timing out and also prevents loss of data
- MPLS VPNs greatly simplify service deployment compared to traditional IP VPNs. As the number of routes and customers increases, MPLS VPNs easily scale, while providing the same level of privacy as Layer 2 technologies. In addition, they can transport non-unique IP addresses across a public domain
- MPLS class-of-service (CoS) capability ensures that important traffic is given the appropriate priority over the network and that latency requirements are met. IP QoS mechanisms can be seamlessly implemented in an MPLS environment

MPLS Mechanisms

Cisco IOS MPLS delivers both traffic engineering (TE) and VPN solutions built on the following mechanisms:

- Cisco AutoBandwidth Allocator: Automatically increases or decreases MPLS TE tunnel bandwidth based on measured traffic load
- Constraint-based Routing Label Distribution Protocol (CR-LDP): A signaling mechanism used to support TE across a MPLS backbone
- Fast Reroute (FRR): Enables quick recovery in case of link failures, which prevents end-user applications from timing out and also prevents loss of data
- Label Distribution Protocol (LDP): Provides communication between edge and core devices. It assigns labels in edge and core devices to establish Label Switched Paths (LSPs) in conjunction with routing protocols such as OSPF, IS-IS, EIGRP, or BGP
- Transmission Control Protocol (TCP): Connection-oriented transport-layer protocol that provides reliable full-duplex data transmission. Part of the TCP/IP protocol stack

For More Information

See the Cisco IOS MPLS Web site: **http://www.cisco.com/go/mpls**

IP Multicast and Multicast Solutions

IP Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients and homes. Applications that take advantage of multicast technologies include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

Multicast technology is key to preventing severe network slowdown and Cisco IOS Multicast is the gateway to Internet broadcasting applications. Internet service providers (ISPs) and content providers use Cisco IOS multicast solutions successfully to host events such as live concerts, radio shows, and football games.

Another application of multicast technologies relates to replacing dedicated point-to-point telephone/voice circuits and specialized bridging and mixing multi-user audio conferencing telephone equipment for "always-on" service (referred to in some industries as "Hoot & Holler" systems). This ability eliminates the need for dedicated, costly, overlay voice networks and point-to-point telephone company circuits, and allows the same capabilities to be implemented over a converged IP network without requiring users to dial in.

Multicast Solutions

Cisco IOS Multicast solutions are classified as Multicast-Lite, Core Multicast, and Enhanced Multicast, and are the building blocks for Internet broadcast. Customers can start with Multicast-Lite, then add more sophisticated interactive communication capabilities, as needed.

- Multicast-Lite provides for one-to-many broadcast capability with no back channel. This solution is eminently suitable for content distribution and broadcasting over the Internet. It does not require setting up of source discovery across domains and autonomous systems. Multicast Lite includes Protocol Independent Multicast version 2 (PIMv2), Internet Group Management Protocol (IGMPv1/v2/v3) or Universal Resource Locator Rendezvous Directory (URD).
- Core Multicast provides interactive, reliable campus multicast for interactive distance learning, corporate videoconferencing, inventory updates, software distribution, and content distribution. Core Multicast includes PIM, IGMP, Cisco Group Management Protocol (CGMP), and now Pragmatic General Multicast (PGM).
- Enhanced Multicast provides interactive Internet Multicast across domains for network gaming, inter-company conferencing, Internet software distribution, and extranet content distribution. Enhanced Multicast includes Multicast Border Gateway Protocol (MBGP) and Multicast Source Discovery Protocol (MSDP) in addition to all the protocols supported in Core Multicast.

Multicast is available across all Cisco IOS Software-based platforms, including Cisco routers and Catalyst family switches. Multicast-supported routing platforms include the following: Cisco 1600, 2500, 2600/2600XM, 3600, 3700, 3800, 7200, 7500, and 12000 series; it also is available on Catalyst 6000 and 8500 platforms.

Multicast Features

Cisco has the greatest depth of experience with IP Multicast in the industry, and offers multicast features such as:

Bi-dir PIM	An extension to the PIM suite of protocols that implements shared sparse trees with bi-directional flow of data.
Cisco Group Management Protocol (CGMP)	Cisco-developed protocol that allows Layer 2 switches to leverage IGMP information on Cisco routers to make Layer 2 forwarding decisions.
Internet Group Management Protocol v2 (IGMP)	Used by IP routers and their immediately connected hosts to communicate multicast group membership states: • Query: IGMP messages originating from the router(s) to elicit multicast group membership information from its connected hosts • Report: IGMP messages originating from the hosts that are joining, maintaining or leaving their membership in a multicast group
Internet Group Management Protocol v3 (IGMP)	Version 3 of IGMP adds support for "source filtering," that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address.
IGMP Snooping	Requires the LAN switch to examine, or "snoop," some Layer 3 information in the IGMP packet sent from the host to the router. When the switch hears an IGMP Report from a host for a particular multicast group, the switch adds the host's port number to the associated multicast table entry. When it hears an IGMP Leave Group message from a host, it removes the host's port from the table entry.
Inter domain Multicast	Supports inter-domain routing and source discovery across the Internet or across multiple domains comprising an enterprise
Intra domain Multicast	Supports multicast applications within an enterprise campus
Multicast Source Discovery Protocol (MSDP)	A mechanism to connect multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) (RPs) in different domains.
Multicast Routing Monitor (MRM)	A management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure
Multi-protocol Extensions for Border Gateway Protocol (MBGP)	Also known as BGP+, MBGP adds capabilities to BGP to enable multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems.
Pragmatic General Multicast (PGM)	A reliable multicast transport protocol for applications that require ordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss.
Protocol Independent Multicast (PIM)	A multicast routing architecture that enables IP multicast routing on existing IP networks: • SM = Spare Mode (RFC 2362): Relies upon an explicitly joining method before attempting to send multicast data to receivers of a multicast group. • DM = Dense Mode (Internet Draft Spec): Actively attempts to send multicast data to all potential receivers (flooding) and relies upon their self-pruning (removal from group) to achieve desired distribution.
Unidirectional Link Routing (UDLR) Protocol	A routing protocol that provides a way to forward multicast packets over a physical unidirectional interface (such as a satellite link of high bandwidth) to stub networks that have a back channel
URL Rendezvous Directory (URD)	Directly provides the network with information about the specific source of a content stream. It enables the network to quickly establish the most direct distribution path from the source to the receiver, thus significantly reducing the time and effort required in receiving the streaming media. URD allows an application to identify the source of the content stream through a web page link or web directly.

For More Information

See the Multicast Web site: **http://www.cisco.com/go/multicast**

IPv6

Internet Protocol version 6 (IPv6), most notably offers expanded IP addresses to accommodate the proliferation of Internet devices such as personal computers, personal digital assistants, wireless devices, and new Internet appliances—and the expansion of Internet access, particularly “always-on” connections throughout the world. IPv6 also provides integrated auto-configuration for “plug-and-play” capabilities, enhanced mobility and end-to-end security.

Incorporating IPv6 into Cisco IOS Software further enables growth of the Internet and expansion into new applications and capabilities, while maintaining compatibility with existing Internet services. Cisco’s IPv6 solution was first made available in Cisco IOS Software Release 12.2(1)T. Platforms supported include: Cisco 800, 1700, 2500, 2600/2600XM, 3600, 7100, 7200, and 7500 Series Routers, and Cisco AS5300 and AS5400 Universal Access Servers.

For more information

See the Cisco IOS IPv6 Web site: **http://www.cisco.com/go/ipv6**

Cisco IOS Software Release Process

There are three categories of Cisco IOS Software releases: Early Deployment, Major, and General Deployment (GD) releases.

- Early Deployment releases (i.e. T, S, X, E release families)—Provide advanced networking technologies to customers for delivery of leading-edge Internet applications. These offer new software capabilities, new platforms, and interface extensions. Customers for whom receiving a new feature is critical to their competitive advantage will benefit from these releases
- Major releases (i.e. Release 12.2)—Consolidate features, platform support, and functionality from early deployment releases, and emphasize stability. Regular maintenance releases do not introduce new functionality or platform support, but provide continuous improvement and greater quality, leading to general deployment
- General Deployment certification (i.e. Release 12.0) Releases—Have had extensive market exposure in a wide range of network environments and are qualified through extensive metrics that analyze stability, software defect trends, and customer satisfaction surveys. Used for major, business-critical applications

At some point, GD releases are replaced by newer releases with the latest networking technologies. A release retirement process has been established with three principal milestones: End of Sales (EOS), End of Engineering (EOE), and End of Life (EOL).

For More Information on Cisco IOS Software

See the Cisco IOS Software Web site: **http://www.cisco.com/go/ios**

Cisco Network Management Overview

Cisco is transforming traditional network management by focusing on the strengths of Internet-based architectures for greater accessibility and simplification of network management tools, tasks, and processes. Cisco's network management strategy calls for a Web-based model with the following characteristics:

- Simplification of tools, tasks, and processes
- Web-level integration with NMS platforms and general management products
- Capable of providing end-to-end solutions for managing routers, switches, and access servers
- Creation of a management intranet by integrating discovered device knowledge with CCO and third-party application knowledge

Cisco Network Management Products

The CiscoWorks product line offers a set of solutions designed to manage the enterprise network. These solutions focus on key areas in the network such as; optimization of the wide area network (WAN), administering switch-based local area networks (LAN), securing remote and local virtual private networks, and measuring service level agreements within all types of networks. The expanding CiscoWorks product line offers the flexibility to deploy end-to-end network management when and where it is needed.

CiscoWorks Small Network Management Solution

CiscoWorks SNMS is a new network management solution aimed at small to medium businesses (SMB), with 20 or fewer switches, routers, hubs and access servers. CiscoWorks SNMS can also monitor non-Cisco IT assets such as servers, applications, services and printers. CiscoWorks SNMS is an ideal solution for companies that need centralized network management to help optimize performance and maximize network productivity.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Small Network Management Solution	• Simple integrated installation, autodiscovery and automated import of devices using SNMP • Standards-based multi vendor management • Reduce the time and complexity of keeping the networks' configuration, software version and connectivity optimized

Also available for small and medium size customers is the CiscoWorks for Windows (CWW). CWW includes all the features above except for CiscoWorks Resource Manager Essentials (Essentials) which provides additional functionality that allows the customer to of build and maintain an up-to-date hardware and software inventory for up to 20 devices in a network.

Key Features

- Monitors and reports on hardware, configuration, and inventory changes
- Provides a wizard-based approach for managing and deploys configuration changes and software image updates to multiple Cisco devices
- Allows configuration changes to be performed against multiple switches or routers in the network
- Provides software update analysis reports showing prerequisites and impacts of proposed updates
- Provides a comprehensive audit of network changes, showing who changed what, when, and how
- Summarizes syslog events by severity or user criteria for switches, routers, and Cisco IOS and PIX firewalls
- Discovery and mapping wizard displays customizable vector-based graphics and hierarchical maps of networked devices

CiscoWorks Small Network Management Solution Components

CiscoWorks Small Network Management Solution includes the following tools:

- CiscoView 5.3—Provides graphical back and front panel views of Cisco devices; dynamic, color-coded graphical displays to simplify device-status monitoring, device-specific component diagnostics, device configuration, and application launching
- WhatsUp Gold 7.0 from Ipswitch, Inc.—Provides network discovery, mapping, monitoring, and alarm tracking
- Resource Manager Essentials 3.3.2—Resource Manager Essentials (RME) provides tools for building and managing network inventory, deploying configuration and software image changes, archiving configurations, and providing an audit trail of network changes

Important: RME has a device limit of 20 or fewer Cisco devices.

Specifications

Feature	CiscoWorks Small Network Management Solution
Hardware Requirements	2 Pentium III or better-based IBM PC or compatible computer, 256 MB RAM total, 4 GB free hard drive space
Software Requirements	Windows 2000 with SP1 or 2 (Professional or Sever), Netscape 4.77, 4.78 or Internet Explorer 5.5 with Service Pack 1

Selected Part Numbers and Ordering Information

CiscoWorks Small Network Management Solution

CWSNM-1.0-WIN	Small Network Management Solution 1.0 for Windows; includes WhatsUp Gold 7.0, Resource Manager Essentials 3.3.2 (20 Cisco Device restriction), CiscoView 5.3

For More Information

See the CiscoWorks Small Network Management Solution Web Site:
http://www.cisco.com/go/wrsnms

CiscoWorks Routed WAN Management Solution

The RWAN solution addresses the needs of managing WANs by improving the accuracy, efficiency, and effectiveness of your network administrators and operations staff while increasing the overall availability of your network through proactive planning, deployment, and troubleshooting tools. The CiscoWorks Routed WAN Management Solution provides increased visibility into network behavior, assists in quickly troubleshooting performance bottlenecks, and provides comprehensive tools to easily administer new software and configuration changes for optimizing bandwidth and utilization across expensive and critical links in the network.

When to Sell

Sell This Product	When a Customer Needs These Features
Routed WAN Management Solution	• Optimize router performance by automatically streamlining access control lists, and applying policy-based changes via templates • Understand the responsiveness of WAN connections to determine where bottlenecks are; provides real-time analysis of end-to-end hop delays • Increase network performance by monitoring traffic of protocols, applications, and interface characteristics • A watchdog system to monitor WAN characteristics • An accurate inventory baseline; including memory, slots, software versions, and boot ROMs needed to make decisions • Automate the process of updating device software and configuration • Graphically displays a devices operational status with tools to monitor its activity or change its configurations • Support for secure browser communications and downloads from CiscoView, RME and ACLM via Secure Socket Layer (SSL) or Secure Shell (SSH) protocol

Key Features

- Access Control List Manager—Provides a wizard and policy template-based approach to simplifying the setup, management, and optimization of Cisco IOS Software-based IP and Internetwork Packet Exchange (IPX) traffic filtering and device access control
- Internetwork Performance Monitor—Used to diagnose latency, identify network bottlenecks, and analyze response times
- Resource Manager Essentials—Provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis
- CiscoView—Provides back- and front-panel displays; dynamic, color-coded graphical displays simplify device-status monitoring, device-specific component diagnostics, and application launching
- CiscoWorks Server—Provides the common management desktop services and security across the CiscoWorks family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications
- Support for secure browser communications with CiscoView and RME sessions via Secure Socket Layer (SSL) and Secure Shell (SSH) protocol

Specifications

Feature	Routed WAN Management Solution Requirements
Server	Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) IBM PC compatible with 550-MHz or higher Pentium III processor running (Dual processor system required for hosting multiple management solutions) Microsoft Windows 2000 Server or Professional Edition with Service Pack 2, Solaris 2.8
Client	IBM PC-compatible computer with 300-MHz or higher Pentium processor, Sun Ultra 10, HP9000 Series, IBM RS/6000 Windows NT 4 (Workstation and Server) with Service Pack 6a, Windows 98, 2000 Professional and Server with Service Pack 2; Solaris 2.7, 2.8; HP-UX 11.0; AIX 4.3.3 IBM PC-compatible computer with 300-MHz or higher Pentium processor, Sun Ultra 10, HP9000 Series, IBM RS/6000
Supported Devices	Most Cisco IOS Software routers, access servers, hubs, and switches
Supported Cisco IOS Software Versions	Generally supports Cisco IOS Software Versions 10.3 and above; Catalyst Supervisor code 2.1 and above Note: Some CiscoWorks applications require specific versions of IOS and CAT these releases in order to operate; please see the specific application documentation and release notes for more information.

Selected Part Numbers and Ordering Information[1]

Cisco Routed WAN Management Solution

CWRW-1.2-K9	Routed WAN Management Solution 1.2 for Windows and Solaris platforms; includes Access Control List Manager 1.4, Internetwork Performance Monitor 2.4, Resource Manager Essentials 3.4, CD One 5th Edition (Includes CiscoView 5.4)
CWRW-1.2-P1-K9	Cross Bundle Discount RWAN 1.2 for Windows and Solaris platforms; available to customers who have previously purchased LMS 1.X or LMS 2.X and want to add RWAN
CWRW-1.2-MR-K9	Maintenance kit for customers that purchased RWAN 1.X and now want new device support and code upgrades; kit includes support for Windows and Solaris platforms; includes updates to all components

[1] This is only a small subset of all parts available via URL listed under "For More Information." Some parts have restricted access or are not available through distribution channels.

For More Information

See the Routed WAN Management Solution Web site: **http://www.cisco.com/go/rwan**

CiscoWorks LAN Management Solution

The CiscoWorks LAN Management Solution consists of operationally focused tools. These tools include fault management, scalable topology views, sophisticated configuration, Layer 2/3 path analysis, voice-supported path trace, traffic monitoring, end-station tracking workflow application servers management, and device troubleshooting capabilities. CiscoWorks LMS combines applications and tools for configuring, monitoring, and troubleshooting the campus network.

When to Sell

Sell This Product	When a Customer Needs These Features
LAN Management Solution	• A set of tools for managing Cisco's award winning Catalyst switches • Time saving user tracking and path trace analysis tools with support of IP phones • Automated process of inventorying network devices, updating device software, and managing configuration to reduce the time and errors involved in network updates • Browser-accessible, graphical tool for configuring and monitoring Cisco device components and operational status • VLAN, ATM, or LANE service management tools • RMON traffic monitoring and analysis capability • Active fault monitoring of Cisco devices

Key Features

- Campus Manager—Web-based applications designed for managing Layer 2 device and connectivity discovery, workflow application server discovery and management, detailed topology views, virtual LAN/LAN Emulation (VLAN/LANE) and ATM configuration, end-station tracking, Layer2/3 path analysis tools, and IP phone user and path information
- Device Fault Manager—Provides real-time fault analysis for Cisco devices, automatically includes Cisco devices into its monitoring environment and applies a Cisco "Best Practices" fault rule to each device
- nGenius Real Time Monitor—Web-enabled multiuser traffic management tool set that provides access to network-wide, real-time RMON information for monitoring, troubleshooting, and maintaining network availability
- Resource Manager Essentials—Provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis
- CiscoView—Provides back- and front-panel displays; dynamic, color-coded graphical displays simplify device-status monitoring, device-specific component diagnostics, and application launching
- CiscoWorks Server—Provides the common management desktop services and security across the CiscoWorks Family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications
- Support for secure browser communications with CiscoView and RME sessions via Secure Socket Layer (SSL) and Secure Shell (SSH) protocol

Specifications

Feature	Description
Server	Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) IBM PC compatible with 550-MHz or higher Pentium III processor running (Dual processor system required for hosting multiple management solutions) Microsoft Windows 2000 Server or Professional Edition with Service Pack 2, Solaris 2.8
Client	IBM PC-compatible computer with 300-MHz or higher Pentium processor, Sun Ultra 10, HP9000 Series, IBM RS/6000 Windows NT 4 (Workstation and Server) with Service Pack 6a, Windows 98, 2000 Professional and Server with Service Pack 2; Solaris 2.7, 2.8; HP-UX 11.0; AIX 4.3.3 Internet Explorer v5.5 with Service Pack 2, 6.0; Netscape 4.76, 4.77, 4.78, 4.79
Supported Cisco Devices	Most Cisco IOS Software routers, access servers, hubs, and switches
Supported Cisco IOS Software Versions	Generally Cisco IOS Software Versions 10.3 and higher Catalyst Supervisor code 2.1 through 4.1 Note: Some CiscoWorks applications require certain versions of IOS and CAT these releases in order to operate, please see the specific application documentation and release notes for more information.

7583 W

Selected Part Numbers and Ordering Information[1]

LAN Management Solution	
CWLMS-2.1-K9	LAN Management Solution 2.1 for Windows and Solaris; includes Campus Manager 3.2, Device Fault Manager 1.2, Resource Manager Essentials 3.4, nGenius Real Time Monitor 1.4, CD One 5th Edition (Includes CiscoView 5.4)
CWLMS-2.1-P1-K9	Cross Bundle Discount LMS 2.1 for Windows and Solaris platforms; available to customers who have previously purchased RWAN 1.X and want to add LMS
LAN Management Solution Upgrades	
CWLMS-2.1-UP-K9	Upgrade kit for LMS 1.X customers wanting to upgrade to LMS 2.1; kit includes support for both Windows and Solaris platforms; primary value of this kit is to provide DFM to LMS 1.X customers
CWLMS-2.1-MR-K9	Maintenance kit for customers that purchased LMS 2.0 and want new device support and code updates; kit includes support for both Windows and Solaris platforms; includes updates to all LMS 2.X components (Should not be purchased by LMS 1.X customers)
CWLMS-1.2-MR-K9	Maintenance kit for customers that purchased LMS 1.X and want new device support and code updates to components in the 1.X release train; DFM is not included

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the LAN Management Solution Web site: **http://www.cisco.com/go/lms**

CiscoWorks VPN/Security Management Solution

CiscoWorks VPN/Security Management Solution (VMS), an integral part of the SAFE Blueprint for network security, combines Web-based tools for configuring, monitoring, and troubleshooting enterprise virtual private networks (VPNs), firewalls, and network and host-based intrusion detection systems (IDS). It offers the ability to monitor remote access links, and IPSec based site to site VPN's links. VMS is a Web-based solution that provides a "dashboard" view of critical VPN resources and their performance, VPN hardware and configuration and troubleshooting reports.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks VPN/Security Management Solution	• Complete management of a SAFE infrastructure environment • Configuring and monitoring VPN, PIX, IOS routers, and IDS devices. • Monitoring large remote access, and site-to-site hub and spoke VPNs from a single management console and focus on problem areas and performance.

Key Features

- Management and Monitoring Centers—Supplies the latest in management functionality and multifaceted scalability by offering features such as a consistent user experience, auto update, command and control workflow, and role-based access control. The management and monitoring centers include Management Center for PIX Firewalls, Management Center for IDS Sensors, Management Center for VPN Routers, and Monitoring Center for Security and Management center for PIX Firewalls (downloadable from CCO Software Center Fall 2002)
- VPN Monitor—Allows network administrators to collect, store, and view information on IPSec VPN connections for remote-access or site-to-site VPN terminations. Multiple devices can be viewed from an easy-to-use dashboard that is configured using a Web browser
- Cisco IDS Host Sensor Console—Provides real-time analysis and reaction to network hacking attempts by identifying an attack and preventing access to critical server resources before any unauthorized transactions occur

- Cisco Secure Policy Manager (CSPM)—Provides scalable, powerful policy-based security management system for Cisco firewalls and IPSec VPN routers which allows a customer to define, distribute, enforce, and audit network-wide security policies from a central location
- Resource Manager Essentials (RME)—Provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis
- CiscoView—Provides back- and front-panel displays; dynamic, color-coded graphical displays simplify device-status monitoring, device-specific component diagnostics, and application launching
- CiscoWorks Server—Provides the common management desktop services and security across the CiscoWorks family of solutions. It also provides the foundation for integrating with other Cisco and third-party applications
- Support for secure browser communications with CiscoView and RME sessions via Secure Socket Layer (SSL) and Secure Shell (SSH) protocol

Specifications

Feature	CiscoWorks VPN/Security Management Solution
Server Hardware Requirements	IBM PC-compatible computer with 1-GHz or faster Pentium processor Sun UltraSPARC 60 MP with 440-MHz or faster processor Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server)
Server Software Requirements	Windows 2000 Professional, Windows 2000 Server (Service Pack 2) Sun Solaris 2.7, 2.8
Client Hardware Requirements	IBM PC-compatible computer with 300-MHz or faster Pentium Solaris SPARCstation or Sun Ultra 10
Client Software Requirements	Windows 98, Windows NT 4.0, or Windows 2000 Server or Professional Edition with Service Pack 2 Solaris 2.7, 2.8
Browser Requirements	Internet Explorer 6.0 or 5.5 with Service Pack 2, on Windows 2000 Server or Professional Edition, Windows 98, and Windows NT 4.0. Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition and Windows 98. Netscape Navigator 4.76 on Solaris 2.7, 2.8.

Selected Part Numbers and Ordering Information

CiscoWorks VPN/Security Management Solution

CWVMS-2.1-UR-K9	CiscoWorks VMS 2.1 Windows and Solaris; Includes: Management Center for IDS Sensors, Management Center for VPN Routers, and Monitoring Center for Security, VPN Monitor 1.2, RME 3.4, CSPM 3.1, IDS Host Sensor 2.1, CD One 5th Edition[1]
CWVMS-2.1-WINR-K9	CiscoWorks VMS 2.1 Windows (20-Device Restricted License); Includes: Management Center for IDS Sensors, Management Center for VPN Routers, and Monitoring Center for Security, VPN Monitor 1.2, RME 3.4, CSPM 3.1, IDS Host Sensor 2.1, CD One 5th Edition
CWVMS-2.1-URC-K9	Conversion from CiscoWorks VMS 2.1 for Windows (20-device Restricted License) to Unrestricted License (add Solaris Versions of CV, RME, VPN, and adds an unrestricted license to CSPM for Windows)[1]
CWVMS-2.1-UPGUR-K9	Upgrade from CSPM 2.x (Unrestricted License) to CiscoWorks VMS 2.1 for Windows and Solaris (Unrestricted License)[1]
CWVMS-2.1-WUPGR-K9	Upgrade from CSPM 2.X (Unrestricted License) to CiscoWorks VMS 2.1 for (20-device Restricted License)
CWVMS-2.1-UR-MR-K9	Maintenance release update for VMS 2.0 Windows and Solaris (Unrestricted License)[1]
CWVMS-2.1-R-MR-K9	Maintenance release update for VMS 2.0 Windows Only (20-device Restricted License)

[1] Contains Windows-only versions of CSPM and IDS Host Sensor

For More Information

See the CiscoWorks VPN/Security Management Solution Web site:
http://www.cisco.com/go/vms

CiscoWorks IP Telephony Environment Monitor

CiscoWorks IP Telephony Environment Monitor (ITEM) is a bundled suite of management applications that helps ensure the manageability of converged networks that support Cisco IP telephony and IP telephony data applications. ITEM tracks the health of Cisco IP telephony environments by proactively monitoring the Cisco elements that support voice in the network to alert operations personnel of potential problems in order to minimize IP telephony service interruption.

7581
3

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks IP Telephony Environment Monitor	• Network managers who need to effectively manage their converged networks while maintaining high confidence that their IP telephony environments are performing as expected • Network Managers who need to use synthetic traffic (replicating key forms of network activity associated with VoIP and IP telephony) to enable around-the-clock monitoring of key voice elements in the network

Key Features

- Cisco Voice Health Monitor (VHM)—tracks the health of Cisco IP telephony environments by proactively monitoring Cisco voice elements in the network to alert operations personnel to potential problems and helps to minimize IP telephony service in network downtime. VHM leverages and requires the services of DFM while providing sophisticated capabilities of its own to ensure timely information on the health of IP telephony environments
- Cisco Device Fault Manager (DFM)—DFM provides real-time fault detection and determination about the underlying Cisco IP fabric on which the IP telephony implementation executes. DFM reports faults that occur on Cisco network devices, often identifying problems before users of network services realize that a problem exists
- CiscoView—CiscoView is a web-based graphical device-management technology and is the standard for managing Cisco devices, and providing back and front panel displays. Features include: Real-time monitoring of key information relating to device performance, traffic, and usage, with metrics such as utilization percentage, frames transmitted and received, errors, and a variety of other device-specific indicators

Optional Drop-In Modules

Fault History Manager

Fault History is an optional drop-in module (downloadable from CCO) that provides a web-based tool to access historical fault and alert data from a database. The user has several filtering options that can facilitate the search for specific information.

IP Phone Information Utility

The IP Phone Information Utility is an optional drop-in module (downloadable from CCO) that provides a web-based tool to show detailed information about individual IP telephone. The operator can access the IP phone information by using its extension number, IP address, and/or MAC address. This utility bases its information on the devices created in VHM.

IP Phone Help Desk Utility

The IP Phone Help Desk Utility is an optional applet (downloadable from CCO) that provides a MS Windows 2000 desktop tool to show summary information about individual IP telephone. The help desk operator can access the IP phone information by using its extension number (or can configure the application to search by IP or MAC addresses). This utility requires a connection to an ITEM server running VHM with the IP Phone Information Utility installed.

Gateway Statistics Utility

When available, the Gateway Statistics Utility is an optional drop-in module (downloadable from CCO) that provides a web-based tool to collect performance and behavior statistics about CCM-controlled IP telephony gateways. This statistical information can be subsequently exported for processing by reporting packages for capacity planning and trending information.

Specifications

Feature	CiscoWorks IP Telephony Environment Manager
Server Hardware	IBM PC-compatible with 1 GHz or higher Pentium IV processor UNIX (If DFM is on Unix platform; Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server) (Dual processor system required for hosting multiple management solutions)
Server Software	Windows 2000 Server or Professional Edition with Service Pack 2 Solaris 2.8
Client	IBM PC-compatible computer with 300 MHz or higher Pentium processor Windows NT 4 (Workstation & Server) with Service Pack 6a, Win 98 or Windows 2000 Professional & Server with Service Pack 2 Windows 98/NT/2000: Netscape v4.77, 4.78, 4.79 Windows 98/NT/2000: Internet Explorer v5.5 with Service Pack 2, 6.0

Selected Part Numbers and Ordering Information

CiscoWorks IP Telephony Environment Monitor

CWITEM-1.3-WIN-K9	CiscoWorks IP Telephony Environment Manager 1.3 for Windows Add-On for existing LMS 2.X and DFM 1.1 customers; includes VHM only
CWITEM-1.3-WIN-UP	CiscoWorks VoIP Health Monitor 1.0 Add-On for existing LMS 2.0 and DFM 1.1 customers; includes VHM only
CWITEM-1.3-MR-K9	Maintenance kit for customers that purchased CiscoWorks VoIP Health Monitor 1.0 and now want the new ITEM 1.3 device support and minor updates; kit includes support for Windows platforms only; includes updates to all components

For More Information

See the CiscoWorks IP Telephony Environment Monitor Web site at:
http://www.cisco.com/go/cwvoip

CiscoWorks Voice Manager for Voice Gateways

CiscoWorks Voice Manager for Voice Gateways (CVM) is a client-server, web-based voice management and reporting solution. The application provides enhanced capabilities to configure and provision voice ports, and create and modify dial plans on voice-enabled Cisco routers for voice over IP (VoIP), voice over Frame Relay (VoFR), and voice over ATM (VoATM) network deployments.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks IP Telephony Environment Monitor	• Network managers who need to maintain a distributed network architecture for increased scalability • Network Managers who need to manage multiple customer networks from one common server

Key Features

- Web interface management of voice ports and dial plan generation and management—Create and manage local dial plans and VoIP, VoFR, and VoATM network dial plans
- Report generation—Enhance graphical reporting capabilities with the software provided by an alliance with Telemate.Net (WIndows NT), a leading developer of enterprise information management tools; optional capabilities for enhanced reports, custom report creation, and multiple data source record collection exists.
- Optional capabilities to provide reporting on other data sources such as private branch exchanges (PBXs) and selected firewalls
- CiscoView—CiscoView is a web-based graphical device-management technology and is the standard for managing Cisco devices, and providing back and front panel displays. Features include: Real-time monitoring of key information relating to device performance, traffic, and usage, with metrics such as utilization percentage, frames transmitted and received, errors, and a variety of other device-specific indicators

7579 3

Specifications

Feature	CiscoWorks Voice Manager for Voice Gateways
Server Hardware Requirements	256 MB of memory; 8-GB available hard disk space CPU running at 450 MHz (for Windows NT) Sun Sparc/Ultra @333 MHz (for Solaris)
Server Software Requirements	Windows NT 4.0 with Service Pack 5 CiscoWorks CD One 4th Edition for Windows NT
Client Hardware Requirements	64 MB of memory CPU running at 300 MHz
Client Software Requirements	Windows 95 running Netscape 4.04 or Internet Explorer 4.01 and 64 MB of virtual memory Windows NT running Netscape 4.04 or Internet Explorer 4.01 and 64 MB of virtual memory Solaris running Netscape 4.04 with Telnet and Java enabled and 64 MB of virtual memory

Selected Part Numbers and Ordering Information[1]

CiscoWorks Voice Manager for Voice Gateways 2.1 9

CWVM-2.1	Voice Manager 2.1 for Windows & Solaris; includes Voice Manager 2.1 and CD One 4th Edition (CiscoView 5.3 and the October 2001 Java patch update)
CWVM-2.1-UPG	Upgrade kit for CWVM 1.X customers wanting to upgrade to CVM 2.1; kit includes support for both Windows and Solaris platforms
CWVM-2.1-UPT	Minor updates to CWVM 2.1 for Windows and Solaris from CWVM 2.X; update includes support for both Windows and Solaris platforms

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels.

For More Information

See the Voice Manager for Voice Gateways Web site at:
http://www.cisco.com/go/cw2kvm

CiscoWorks QoS Policy Manager

QoS Policy Manager allows you to centrally define and administer IOS and CAT parameters needed for differentiating network traffic. This ensures high availability and predictable performance for business-critical which rely on advanced voice and video services. Cisco QoS Policy Manager (QPM) 3.0 is a key enabler of end-to-end QoS for converged networks. It delivers differentiated services across network infrastructures with converged voice, video, and data applications, simply by taking advantage of Cisco IOS and Catalyst OS Software with built-in QoS mechanisms in LAN and WAN switching and routing equipment.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco QoS Policy Manager	• End-to-end QoS configuration and automated, reliable policy deployment, while eliminating device-by-device command streams • Rules-based policies that combine static and dynamic port applications and host system traffic filters • QoS Policy Manager's services, including congestion management & avoidance, and traffic-shaping • Efficiently translate policies to specific QoS config commands, ensuring consistency across domains • Validate policies prior to deploying them quickly and reliably to LAN and WAN policy domains • Generate Web-based reports on QoS policies deployed in the network

Key Features

- Provides baseline monitoring which profiles traffic by top applications and a small number of classes before QoS deployment
- Validates QoS deployments by obtaining detailed feedback on traffic patterns after QoS at different points in the network
- Provides statistics related to QoS policies which include traffic matching NBAR filters and action statistics
- Supports CBQoSMIB and CAR MIB
- IP Telephony templates provide pre-defined QoS policies that ensure strict priority for voice traffic in Enterprise networks
- Delivers the appropriate service-level to business-critical applications by supporting the extension of IP packet classification to include application signature, Web URLs, and negotiated ports
- Extend security by defining access control policies to permit or deny transport of packets into or out of device interfaces
- Allows QoS policy validation checking, uploading of existing device configuration, previewing configuration changes, incremental ACL updates, and managing policy distribution

Specifications

Feature	Cisco QoS Policy Manager
Server Hardware Requirements	IBM PC-compatible computer with 1-GHz or faster Pentium processor Sun UltraSPARC 60 MP with 440-MHz or faster processor Sun UltraSPARCIII (Sun Blade 1000 Workstation or Sun Fire 280R Workgroup Server)
Server Software Requirements	Windows 2000 Professional, Windows 2000 Server (Service Pack 2) Sun Solaris 2.7, 2.8
Client Hardware Requirements	IBM PC-compatible computer with 300-MHz or faster Pentium Solaris SPARCstation or Sun Ultra 10Complete
Client Software Requirements	Windows 98, Windows NT 4.0, or Windows 2000 Server or Professional Edition with Service Pack 2 Solaris 2.7, 2.8
Browser Requirements	Internet Explorer 6.0 or 5.5 with Service Pack 2, on Windows 2000 Server or Professional Edition, Windows 98, and Windows NT 4.0. Netscape Navigator 4.79, on Windows 2000 Server or Professional Edition and Windows 98, Netscape Navigator 4.76 on Solaris 2.7, 2.8.

Selected Part Numbers and Ordering Information[1]

Cisco QoS Policy Manager

CWQPM-3.0-WINUR-K9	QoS Policy Mgr 3.0 for Windows (Unrestricted License)
CWQPM-3.0-WINR-K9	QoS Policy Mgr 3.0 for Windows (20- Device Restricted License)
CWQPM-3.0-URUP-K9	Upgrade to QPM 3.0 for Windows from QPM 1.x or 2.x to QPM 3.0 unrestricted
CWQPM-3.0-URC-K9	Conversion of a QPM 3.0 20-device restricted usage license to unrestricted device usage license

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco QoS Policy Manager Web site: **http://www.cisco.com/go/qpm**

Cisco Ethernet Subscriber Solution Engine

The Cisco Ethernet Subscriber Solution Engine (ESSE) is a hardware-based management system for metro access networks that use the Cisco ONT 1000 Gigabit Ethernet Series Optical Network Terminator. The Cisco ESSE enables complete remote management and troubleshooting of the customer demarcation point for Ethernet over fiber. Remote management and diagnostics reduce operating expenses and increase profitability by eliminating the need for unnecessary visits to the customer premises. The Cisco ESSE runs on the Cisco 1105, which is one rack unit (1RU) high, enabling you to conveniently deploy the Cisco ESSE on the same rack with the rest of your Cisco metro Ethernet network aggregation equipment.

The Cisco ESSE automatically discovers all Cisco ONT 1000 Gigabit Ethernet Series devices in the metro access network, applies the designated configuration, and instantly begins collecting statistics and management information.

When to Sell

Sell This Product	When a Customer Needs These Features
Cisco Ethernet Subscriber Solution Engine	The Cisco Ethernet Subscriber Solution Engine is ideal for service providers seeking to: • Reduce operating expenses by implementing metro access networks with Ethernet over fiber • Reduce customer onsite visits, which are time-consuming and expensive • Perform complete remote configuration and troubleshooting of the Cisco ONT 1000 Gigabit Ethernet Series

Key Features

- Enables service providers to perform remote control of inventory, configuration, statistics, fault management, and troubleshooting on the Cisco ONT 1000 Gigabit Ethernet Series
- Full Layer 1 and Layer 2 remote configuration and monitoring of Optical Network Terminators
- Access to all Ethernet port registers and statistics on the Cisco ONT 1000 Gigabit Ethernet Series
- Easy identification of ONTs with searchable, user-defined properties such as customer name, VLAN ID, and street address

Selected Part Numbers and Ordering Information[1]

Cisco Ethernet Subscriber Solution Engine	
CESSE-1105-K9	Cisco Ethernet Subscriber Solution Engine; Includes the Cisco 1105 hardware platform and Ethernet Subscriber management software, version 1.1

[1] This is only a small subset of all parts available via URL listed under "For More Information". Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the Cisco Ethernet Subscriber Solution Engine Web site:
http://www.cisco.com/go/esse

CiscoWorks Wireless LAN Solution Engine

The CiscoWorks WLSE is a specialized, daily operational solution that allows customers to manage the entire Cisco Aironet WLAN infrastructure. It offers powerful, centralized template-based configuration with user-defined device groups to efficiently configure large numbers of access points and bridges. The CiscoWorks WLSE provides centralized firmware updates to facilitate firmware changes throughout the WLAN. It monitors Access Control Server (ACS) authentication servers, supports both Cisco Extensible Authentication Protocol (LEAP) and generic RADIUS servers, and further enhances security management by detecting misconfigurations on access points and bridges. The CiscoWorks WLSE proactively monitors WLAN infrastructures and generates notifications for unavailability and performance degradation. The CiscoWorks WLSE aids in capacity planning by identifying the most used access points, and accelerates troubleshooting by generating client association reports.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Wireless LAN Solution Engine	The CiscoWorks WLSE is ideal for enterprise customers: • Implementing large-scale Cisco Aironet WLAN infrastructures • Template-based configuration tool which can include a large number of uniform policies for Cisco access points and bridges • Access point and bridge mis-configuration alerts to minimize security vulnerabilities • Proactive fault and performance monitoring of Cisco access points, bridges, LEAP authentication server, and switches connected to the access points

Key Features

- Centralized template-based configuration with hierarchical, user-defined groups
- Plug and play configuration of newly deployed access points and bridges
- Centralized firmware update to facilitate firmware changes
- Access point and bridge misconfiguration alerts to minimize security vulnerabilities
- Proactive monitoring of access points, bridges, ACS authentication servers (both LEAP and generic RADIUS), and the switches connected to the access points
- Configuration and monitoring of virtual LAN (VLAN) and quality of service (QoS) on access points to maximize security and performance
- Access point usage, summary, and client association reports with XML, CSV, and PDF data export
- Secure HTML-based user interface for easy access anywhere
- Upper-layer network management system and operations support system (NMS/OSS) integration with syslog message, SNMP trap, and e-mail notifications

Selected Part Numbers and Ordering Information[1]

CiscoWorks Wireless LAN Solution Engine	
CWWLSE-1105-K9	Wireless LAN Solution Engine1.0; includes the Cisco 1105 hardware platform and wireless LAN management software version 1.0

For More Information

See the CiscoWorks Wireless LAN Solution Engine Web site: **http://www.cisco.com/go/wlse**

CiscoWorks Hosting Solution Engine

CiscoWOrks Hosting Solution Engine is a network management appliance that monitors, activates, and configures a variety of e-business services in Cisco powered data centers. It provides up-to-date fault and performance information about the network infrastructure and Layer 4-7 network services.

HSE automatically discovers the entire data center infrastructure and instantly begins collecting statistics and management information, providing a current snapshot of the managed environment. HSE provides up-to-date information for operational staff to easily pinpoint the source of a problem. HSE itself is a manageable Cisco device with a full Cisco Discovery Protocol implementation and supports Cisco MIB II.

When to Sell

Sell This Product	When a Customer Needs These Features
CiscoWorks Hosting Solution Engine	• Ideal for enterprise and service providers with e-business data center facilities • Granular user access model to partition network resources for Layer 4-7 services and switch ports, and authorize user group access to individual application services • Robust Layer 4-7 service configuration and service activation of server load balancing devices, including virtual servers, real servers, and content owners and rules

Key Features

- Granular user access to partition network resources for Layer 4-7 services as well as switch ports; authorize user group access to individual application services
- Robust Layer 4-7 service configuration and service activation of content switches
- Monitoring and reporting of SSL Proxy services on Cisco Catalyst 6000 Series with SSL Service Modules and Cisco Content Services Switch
- Flexible fault and performance monitoring of Cisco routers, switches, Cisco PIX® Firewalls, Cisco Content Engines, Cisco Content Switches and L4-7 services
- HTML-based, secure graphic user interface with easy customer view/report personalization and historical data reporting
- Upper layer NMS/OSS integration with SYSLOG, trap, email notifications and historical data XML export

Selected Part Numbers and Ordering Information[1]

Cisco 1105 Hosting Solution Engine	
CWHSE1105-1.5-K9	CiscoWorks Hosting Solution Engine; includes 1105 hardware platform with software version 1.5; can be configured for international power cords

[1] Some parts have restricted access or are not available through distribution channels. Resellers: For latest part number and pricing info, see the *Distribution Product Reference Guide* at: http://www.cisco.com/dprg (limited country availability).

For More Information

See the 1105 Hosting Solution Engine Web site: **http://www.cisco.com/go/1105hse**

Cisco Catalyst 6500 Series Network Analysis Module 1 and 2(with NAM software version 2.2)

The Cisco Network Analysis Module (NAM) 1 and 2, second generation high performance network analysis modules for the Cisco Catalyst 6500 Series provides network monitoring instrumentation and web-browser based traffic analysis for Catalyst based AVVID environments. The NAM enables network managers to gain application-level visibility into network traffic with the ultimate goal of improving performance, reducing failures, and maximizing returns on network investment. The new NAMs are available in two hardware versions, NAM-1 and NAM-2, to meet diverse network analysis needs in a scalable switching environment running up to gigabit speeds. The NAMs come with an embedded, Web-based traffic analyzer, which provides full scale remote monitoring and troubleshooting capabilities that are accessible through a Web browser.

When to Sell

Sell This Product	When a Customer Needs These Features
Catalyst 6500 Series Network Analysis Module 1 and 2 (with NAM software version 2.2)	• Needs Application-Level visibility built into the network • Provides network managers visibility into all layers of network traffic • Monitoring in a scalable switching environment that supports traffic monitoring in a scalable switching environment • Offers investment protection by interfacing with both the bus and the crossbar switching fabric-based architectures in the Cisco Catalyst 6500 Series

Key Features

- Provides application-level Remote Monitoring (RMON) functions based on RMON2 and other advanced Management Information Bases (MIBs)
- Collects statistics on both data and VoIP streams flowing through the host switch using the Switch Port Analyzer (SPAN) and NetFlow Data Export features of the Cisco Catalyst 6500 Series
- Collects data from remote switches using the remote SPAN (RSPAN) feature of the Cisco Catalyst 6500 and 4000 Series switches
- Easy to deploy and use at LAN aggregation where they can see most of the traffic, at service points where performance is critical and at important access points where quick troubleshooting is required
- Application monitoring can be done using RMON, RMON2, and several extended RMON MIBs, which can detect the applications on the network and provide detailed information about how these applications utilize the bandwidth, which hosts access those applications, and which client/server pairs generate the most traffic
- Performance management provides valuable information about the delays in server responses to client requests

Selected Part Numbers and Ordering Information[1]

Cisco Catalyst 6500 Series Network Analysis Module 1 and 2(with NAM software version 2.2)

WS-SVC-NAM-1	Catalyst 6500 Series Network Analysis Module 1. To order the NAM individually, please use the spare part number of WS-SVC-NAM-1=
WS-SVC-NAM-2	Catalyst 6500 Series Network Analysis Module 2. To order the NAM individually, please use the spare part number of WS-SVC-NAM-2=

[1] Some parts have restricted access or are not available through distribution channels.

For More Information

See the Cisco NAM Web site: **http://www.cisco.com/go/6000nam**

Ap 6H

CISCO SYSTEMS

Software Advisor

Close Window

Toolkit: Roll over tools below

Feedback | Help

HOME SOFTWARE SUPPORT FOR FEATURES SOFTWARE SUPPORT FOR HARDWARE

Search By Features | **Search By Release** | Compare Releases

Major Release	12.2T
Product Family	3745
Releases	12.2(15)T
Feature Set	IP/FW/IDS PLUS IPSEC 3DES

Some features are dependent on product model, interface modules (i.e. Line Cards & Port Adapters), and/or require a software feature license.

Your selections are supported by the following

Image Name	DRAM	Flash	Product Number	Options
c3745-ik9o3s-mz.12.2-15.T	128	32	S374CHK9-12215T= S374CHK9-12215T	Search For MIBs Compare Images

AAA Broadcast Accounting
AAA DNIS Map for Authorization
AAA Resource Accounting
AAA Server Group
AAA Server Group Deadtimer
AAA Server Group Enhancements
AAA Server Groups Based on DNIS
AAA-PPP-VPDN Non-Blocking
Ability to Disable Xauth for Static IPsec Peers
Accounting of VPDN Disconnect Cause
ACL Authentication of Incoming RSH and RCP
ACL Default Direction
Adaptive Frame Relay Traffic Shaping for Interface Congestion
Additional Vendor-Proprietary RADIUS Attributes
ADSL - Asymmetric Digital Subscriber Line Support
Advanced Encryption Standard (AES)
Advanced Voice Busyout (AVBO)
Airline Product Set (ALPS)
Airline Product Set Enhancements (MATIP)
Always On Dynamic ISDN (AO/DI)
Analog Centralized Automatic Message Accounting E911 Trunk
Answer Supervision Reporting
Asynchronous Line Monitoring
Asynchronous Rotary Line Queuing
ATM Cell Loss Priority (CLP) Setting
ATM LANE Fast Simple Server Redundancy Protocol (LANE Fast SSRP)
ATM SVC Troubleshooting Enhancements
ATM-DXI
Authentication Proxy Accounting for HTTP
AutoInstall Using DHCP for LAN Interfaces
Automatic modem configuration
Bandwidth Allocation Control Protocol (BACP)
BGP

BGP 4
BGP 4 Multipath Support
BGP 4 Prefix Filter and In-bound Route Maps
BGP 4 Soft Config
BGP Conditional Route Injection
BGP Hide Local-Autonomous System
BGP Link Bandwidth
BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN
BGP Named Community Lists
BGP Policy Accounting
BGP Prefix-Based Outbound Route Filtering
BGP Soft Reset
Bidirectional PIM
BIP - BSC to IP Conversion for Automated Teller Machines
Bisync (BSC)
Bridging between IEEE 802.1Q vLANs
Broadcast/Multicast Suppression
BSTUN (Block Serial Tunneling)
Busyout Monitor
Call Admission Control for H.323 VoIP Gateways
Caller ID
CEF on Multipoint GRE Tunnels
CEF Support for IP Routing between IEEE 802.1Q vLANs
CEF/dCEF - Cisco Express Forwarding
CEFv6/dCEFv6 - Cisco Express Forwarding
Certificate Auto-Enrollment
Certificate Enrollment Enhancements
Certification Authority Interoperability (CA)
CGMA - Cisco Gateway Management Agent
CGMP - Cisco Group Management Protocol
Challege Handshake Authentication Protocol (CHAP)
Channelized E1 Signaling
Circuit Interface Identification Persistence for SNMP
Cisco Discovery Protocol (CDP)
Cisco Discovery Protocol (CDP) - IPv6 Address Family Support for Neighbor I...
Cisco IOS Telephony Service (ITS) Version 2.0
Class Based Ethernet CoS Matching & Marking (802.1p & ISL CoS)
Class Based Weighted Fair Queuing (CBWFQ)
Class-Based Frame-Relay DE-Bit Matching and Marking
Class-Based Packet Marking
Class-Based Packet Shaping
Classless InterDomain Routing (CIDR) IP Default Gateway
CLI String Search
ClickStart
CNS Agents SSL Security
CNS Configuration Agent
CNS Event Agent
Commented IP Access List Entries
Committed Access Rate (CAR)
Compression Control Protocol
Configurable per ATM-VC Hold Queue size
Configurable Timers in H.225
Connect-Info RADIUS Attribute 77
Context-Based Access Control (CBAC)
Control Plane DSCP Support for RSVP
COPS for RSVP
Crashinfo Support
CT1/RBS (Robbed Bit Signaling)
CUG Selection Facility Suppress Option
Custom Queueing (CQ)
Customer Profile Idle Timer Enhancements for Interesting Traffic
Default Passive Interface
DF Bit Override Functionality with IPSec Tunnels
DHCP Client
DHCP Client - Dynamic Subnet Allocation API
DHCP Client on WAN Interfaces
DHCP Option 82 Support for Routed Bridge Encapsulation

DHCP Proxy Client
DHCP Relay - MPLS VPN Support
DHCP Relay Agent Support for Unnumbered Interfaces
DHCP Server Options - Import and Autoconfiguration
DHCP Server-Easy IP Phase 2
Dial backup
Dial on Demand Authentication Enhancements
Dial Peer Enhancements
Dial-on-demand
Dialer CEF
Dialer Idle Timer Inbound Traffic Configuration
Dialer Persistent
Dialer profiles
Dialer Watch
Dialer Watch Connect Delay
Diffie-Hellman Group 5
Diffserv Compliant WRED
Digital J1 Voice Support
Direct Inward Dial (DID)
Disabling LANE Flush Process
Distinguished Name Based Crypto Maps
Distributed Management Event MIB Persistence
Distributed Management Expression MIB persistence
DLSw (RFC 1795)
DLSw CO features
DLSw V2
DLSw+
DLSw+ Asynchronous TCP Enhancements
DLSw+ Backup Peer Extensions for Encapsulation Types
DLSw+ Border Peer Caching
DLSw+ Enhanced Load Balancing
DLSw+ Ethernet Redundancy
DLSw+ Peer Group Clusters
DLSw+ RSVP Bandwidth Reservation
DLSw+ SNA Type of Service
DLSw+ Support For Transporting LLC1 UI Traffic
DNS based X.25 routing
DNS Lookups over an IPv6 Transport
Double Authentication
Down Stream Physical Unit (DSPU) over DLSw+
Downstream PU concentration (DSPU)
DRP Server Agent
DTMF Events Through SIP Signaling
Dynamic Multiple Encapsulation for Dial-in over ISDN
E1 R2 Signaling
Easy IP (Phase 1)
Easy VPN Server
Encrypted Vendor Specific Attributes
Enhanced Codec support for SIP using Dynamic Payloads
Enhanced IGRP (EIGRP)
Enhanced IGRP Stub Routing
Enhanced Local Management Interface (ELMI)
Enhanced Password Security
Enhanced Test Command
Express RTP and TCP Header Compression
Fast Fragmentation (Fast-Switched Fragmented IP Packets)
Fast-Switched Compressed RTP
Fast-Switched Policy Routing
Fast-Switched SRTLB
Fax Relay Packet Loss Concealment
Feature Group D Support
Firewall Authentication Proxy
Firewall Feature Set
Firewall Intrusion Detection System
Flow-Based WRED
Frame Relay
Frame Relay - Multilink (MLFR-FRF.16)

7569
3

Frame Relay 64-bit Counters
Frame Relay Access Support (FRAS) Border Access Node (BAN)
Frame Relay Access Support (FRAS) Boundary Network Node (BNN)
Frame Relay Access Support (FRAS) Dial Backup over DLSW+
Frame Relay Access Support (FRAS) DLCI Backup
Frame Relay Access Support (FRAS) Host
Frame Relay ELMI Address Registration
Frame Relay Encapsulation
Frame Relay End-to-End Keepalive
Frame Relay Fragmentation (FRF.12)
Frame Relay Fragmentation with Hardware Compression
Frame Relay FRF.9 Payload Compression
Frame Relay IP RTP Priority
Frame Relay Point-Multipoint Wireless
Frame Relay PVC Interface Priority Queueing
Frame Relay Router ForeSight
Frame Relay Switching
Frame Relay Switching Diagnostics and Troubleshooting
Frame Relay Switching Enhancements: Shaping and Policing
Frame Relay Traffic Shaping (FRTS)
Frame Relay Tunnel Switching
FUNI Support for Routers
FXO Answer and Disconnect Supervision
Gatekeeper Ecosystem Interoperability
Generic Routing Encapsulation (GRE)
Generic Routing Encapsulation (GRE) Tunnel Keepalive
Generic Traffic Shaping (GTS)
H.323 Call Redirection Enhancements
H.323 Dual Tone Multifrequency (DTMF) Relay Using Named Telephone Events
H.323 Redundant Zone Support
H.323 Scalability and Interoperability Enhancements for Gateways
H.323 Support for Virtual Interfaces
Half bridge/half router for CPP and PPP
Hoot and Holler over IP
HSRP - Hot Standby Router Protocol
HSRP - Hot Standby Router Protocol and IPSec
HSRP over ISL
HSRP support for ICMP Redirects
HSRP support for MPLS VPNs
iBGP Multipath Load Sharing
IEEE 802.1Q ISL VLAN Mapping
IEEE 802.1Q Tunneling
IEEE 802.1Q VLAN Support
IEEE 802.1Q VLAN Trunking
IEEE 802.3x Flow Control
IGMP Fast Leave
IGMP MIB Support Enhancements for SNMP
IGMP Snooping
IGMP Version 3
IGMP Version 3 - Explicit Tracking of Hosts, Groups, and Channels
IKE - Initiate Aggressive Mode
IKE Extended Authentication (Xauth)
IKE Mode Configuration
IKE Security Protocol
IKE Shared Secret Using AAA Server
Integrated routing and bridging (IRB)
Inter-Domain Gateway Security Enhancement
Interactive Voice Response (IVR) Version 2.0
Interface Alias Long Name Support
Interface Index Display
Interface Index Persistence
Interface Range Specification
Internal Cause Code Consistency between SIP and H.323
Interworking Signaling Enhancements for H.323 and SIP VoIP
Inverse Multiplexing over ATM (IMA)
IP DSCP marking for Frame-Relay PVC
IP Enhanced IGRP Route Authentication

IP Header Compression Enhancement - PPPoATM and PPPoFR Support
IP Multicast Load Splitting across Equal-Cost Paths
IP Multicast Multilayer Switching (MLS)
IP Multilayer Switching (IP MLS)
IP Named Access Control List
IP Precedence Accounting
IP Precedence for GRE Tunnels
IP Routing
IP RTP Priority
IP Summary Address for RIPv2
IP to ATM CoS, per-VC WFQ and CBWFQ
IP-to-ATM CoS
IPSec MIB Support for Cisco IPSec VPN Management
IPSec Network Security
IPSec Triple DES Encryption (3DES)
IPSec VPN High Availability Enhancements
IPv6 Extended Access Control List
IPv6 for Cisco IOS Software
ISDN
ISDN Advice of Charge (AOC)
ISDN Caller ID Callback
ISDN Cause Code Override
ISDN LAPB-TA
ISDN Leased Line at 128kbps
ISDN Network Side for ETSI Net5 PRI
ISDN NFAS
ISDN Progress Indicator support for SIP using 183 Session Progress
ISDN-NFAS with D Channel Backup
ISL VLAN
IVR: Enhanced Multilanguage Support
L2TP Dial-Out
L2TP Layer 2 Tunneling Protocol
L2TP Security
L2TP Tunnel Preservation of IP TOS
LAN Network Manager over DLSw+
LANE dCEF
LANE Optimum Switching
Large Scale Dialout (LSDO)
Layer 2 Forwarding-Fast Switching
Line Printer Daemon (LPD)
Link Fragmentation and Interleaving (LFI) for Frame Relay and ATM Virtual C...
Local Area Transport (LAT)
Local Voice Busyout (LVBO)
Lock and Key
Low Latency Queueing (LLQ)
Low Latency Queueing (LLQ) for Frame Relay
Low Latency Queueing (LLQ) with Priority Percentage Support
LSDO: L2TP Large-Scale Dial-Out
MAC Address Filtering
MD5 File Validation
Message Banners for AAA Authentication
MGCP - Media Gateway Control Protocol
MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles
MGCP Based Fax (T.38) and DTMF Relay
MGCP Basic CLASS and Operator Services
MGCP CAS PBX and AAL2 PVC
MGCP Generic Configuration Support for Call Manager (IP-PBX)
MGCP PRI backhaul and T1-CAS support for Call Manager (IP-PBX)
MGCP Standalone Remote Office Support for Call Manager (IP-PBX)
MGCP VoIP Call Admission Control
MGCP VoIP Signaling
Microsoft Point-to-Point Compression (MPPC)
Mobile IP
Mobile IP - Mobile Networks
Mobile IP Home Agent (HA) Redundancy
Modem over BRI
Modem PassThrough over Voice over IP

Modem Relay Support on VoIP Platforms
Modem Script and System Script Support in LSDO
Modem User Interface Option
Modular QoS CLI (MQC)
MS Callback
MS-CHAP Version 1
Multi-Chassis Hunting for Voice over Frame Relay
Multicast BGP (MBGP)
Multicast Music on Hold support for Call Manager (IP-PBX)
Multicast NAT
Multicast Routing Monitor (MRM)
Multicast Source Discovery Protocol (MSDP)
Multichassis MultiLink PPP (MMP)
Multihop VPDN
Multilink PPP
Multilink PPP Enable/Disable via Radius for Preauthentication User
Multiple RSA Keypair Support
Multiprotocol over ATM (MPOA)
Multiprotocol over ATM for Token Ring (MPOA)
Named Method Lists for AAA Authorization and Accounting
NAT - Static Mapping Support with HSRP for High-Availability
NAT Stateful Fail-over of Network Address Translation
NAT-Ability to use Routes Maps with Static Translations
NAT-Enhanced H.225/H.245 Forwarding Engine
NAT-Network Address Translation
NAT-Support for NetMeeting Directory (Internet Locator Service - ILS)
NAT-Support for SIP
NAT-Support of H.323v2 Call Signaling (FastConnect)
NAT-Support of H.323v2 RAS
NAT-Support of IP Phone to Cisco Call Manager
NAT-Translation of external IP Addresses only
National ISDN Switch Types for BRI and PRI Interfaces
Native Client Interface Architecture (NCIA) Server
Native Service Point over DLSW+
NBAR - Network-based Application Recognition
NBAR Real-time Transport Protocol Payload Classification
Netflow
NetFlow Aggregation
Netflow Multiple Export Destinations
NetFlow Policy Routing (NPR)
NetFlow ToS-Based Router Aggregation
Network Side ISDN PRI Signaling, Trunking, and Switching
Network Time Protocol (NTP)
Next Hop Resolution Protocol (NHRP)
NFAS Enhancements
Offload Server Accounting Enhancement
On Demand Routing (ODR)
Optimized PPP Negotiation
OSP Debug Enhancement
OSPF
OSPF ABR type 3 LSA Filtering
OSPF Flooding Reduction
OSPF Not-So-Stubby Areas (NSSA)
OSPF On Demand Circuit (RFC 1793)
OSPF Packet Pacing
OSPF Sham-Link Support for MPLS VPN
OSPF Stub Router Advertisement
OSPF Support for Multi-VRF on CE Routers
OSPF Update Packet-Pacing Configurable Timers
PAD Subaddressing
Parse Bookmarks
Parser Cache
Password Authentication Protocol (PAP)
Per-User Configuration
PIM Dense Mode State Refresh
PIM MIB Extension for IP Multicast
PIM Multicast Scalability

PIM Version 1
PIM Version 2
Policer Enhancement - Multiple Actions
Policy-Based Routing (PBR)
Port to Application Mapping (PAM)
PPP
PPP over ATM
PPP over ATM (IETF-Compliant)
PPP over ATM SVCs
PPP Over Fast Ethernet 802.1Q
PPP over Frame Relay
PPPoA/PPPoE autosense for ATM PVCs
PPPoE Client
PPPoE on Ethernet
PPPoE over Gigabit Ethernet interface
PPPoE Radius Port Identification
PPPoE Session limit
Pre-fragmentation For Ipsec VPNs
Preauthentication with ISDN PRI and Channel-Associated Signalling Enhanceme...
PRI/Q.931 Signaling Backhaul for Call Agent Applications
Priority Queueing (PQ)
Protocol Translation (PT)
PSTN Fallback
QoS Device Manager (QDM)
QoS for Virtual Private Networks
QoS Packet Marking
QSIG Protocol Support
Qualified Logical Link Control (QLLC)
RADIUS
RADIUS Attribute 44 (Accounting Session ID) in Access Requests
RADIUS Attribute 66 (Tunnel-Client-Endpoint) Enhancements
RADIUS Attribute 82: Tunnel Assignment Id
RADIUS Attribute Value Screening
RADIUS for Multiple User Datagram Protocol Ports
RADIUS Packet of Disconnect
RADIUS Progress Codes
RADIUS Route Download
RADIUS Tunnel Attribute Extensions
RADIUS Tunnel Preference for Load Balancing and Fail-over
Random Early Detection (RED)
Redial Enhancements
Redundant Link Manager (RLM)
Reflexive Access Lists
Remote Source-Route Bridging (RSRB)
Resource Pool Management with Direct Remote Services
Response Time Reporter (RTR)
Response Time Reporter (RTR) enhancements
Reverse Route Injection (RRI)
RFC 1483 for Token Ring Networks
RGMP - Router-Port Group Management Protocol
RIF Passthru in DLSw+
RIP
RMON events and alarms
Rotating Through Dial Strings
RSVP - ATM Quality of Service (QoS) Interworking
RSVP - Resource Reservation Protocol
RSVP Scalability Enhancements
RSVP Support for Frame Relay
RSVP support for LLQ
RTP Header Compression
SDLC SNRM Timer and Window Size Enhancements
SDLC-to-LAN conversion (SDLLC)
Secure Copy (SCP)
Secure Shell SSH Support over IPv6
Secure Shell SSH Terminal-line access
Secure Shell SSH Version 1 Integrated Client
Secure Shell SSH Version 1 Server Support

4565
3

Selective Packet Discard (SPD)
Selective Virtual-Access Interface Creation
Service Assurance Agent (SAA) APM Application Performance Monitor
Service Assurance Agent (SAA) FTP Operation
Settlement for Packet Telephony
Settlement for Packet Telephony - Roaming & PKI Multiple Roots
Shell-Based Authentication of VPDN Users
Single Rate 3-Color Marker for Traffic Policing
SIP - Call Transfer Using Refer Method
SIP - Configurable PSTN Cause Code Mapping
SIP - DNS SRV RFC2782 Compliance
SIP - Enhanced Billing Support for Gateways
SIP - Session Initiation Protocol for VoIP
SIP - Session Initiation Protocol for VoIP Enhancements
SIP Carrier Identification Code
SIP Diversion Header Implementation for Redirecting Number
SIP Gateway Support for the Bind Command
SIP Gateway support for Third Party Call Control
SIP INFO Method for DTMF Tone Generation
SIP Intra-gateway Hairpinning
SIP INVITE Request with Malformed Via Header
SIP Multiple 18x Responses
SIP Session Timer Support
SIP T.37 and Cisco Fax
SIP T.38 Fax Relay
Snapshot routing
SNMP (Simple Network Management Protocol)
SNMP Inform Request
SNMP Manager
SNMP Support for IOS vLAN Subinterfaces
SNMP Support for vLAN (ISL, DOT1Q) Subinterfaces
SNMP Support over VPN
SNMP Version 3
SNMPv2C
Source Specific Multicast (SSM)
Source Specific Multicast (SSM) - IGMPv3,IGMP v3lite, and URD
Spanning Tree Protocol (STP)
Spanning Tree Protocol (STP) - Backbone Fast Convergence
Spanning Tree Protocol (STP) - Portfast Guard
Spanning Tree Protocol (STP) - Uplink Fast Convergence
Spanning Tree Protocol (STP) Extension
SRB - Source-Route bridging
SRB over Frame Relay
SRST: Survivable Remote Site Telephony Version 2.0
SSRP for LANE
Stack Group Bidding Protocol (SGBP)
Standard IP Access List Logging
Static Cache Entry for IPv6 Neighbor Discovery
Stream Control Transmission Protocol (SCTP)
Stub IP Multicast Routing
STUN (Serial Tunnel)
Subnetwork Bandwidth Manager (SBM)
Switch Port Analyzer (SPAN)
Switch Port Analyzer (SPAN) - Disable Receive Traffic Destination Port
Switch Port Analyzer (SPAN) - Multiple Source Port Selection
Switched Multimegabit Data Service (SMDS)
T.37 Store and Forward Fax
T.37/T.38 Fax Gateway
T.38 Fax Relay for VoIP H.323
Tacacs SENDAUTH function
Tacacs Single Connection
TACACS+
TCL IVR 2.0 Call Initiation and Callback
TCL IVR Disconnect Cause-Code Manipulation
TCP Window Scaling
Time-Based Access Lists Using Time Ranges
Timer and Retry Enhancements for L2TP and L2F

Token Ring ISL
Token Ring LANE
Traffic Policing
Transparent Bridging
Transparent CCS and Frame Forwarding Enhancements
Transparent Common Channel Signaling (T-CCS)
Triggered RIP
Trimble Palisade NTP Synchronization Driver
Trunk Conditioning for FRF.11 and Cisco Trunks
Trusted Root Certification Authority
Trustpoint CLI
Tunnel Endpoint Discovery
Tunnel Type of Service (TOS)
Tunneling of Asynchronous Security Protocols
Turbo Flooding of UDP Datagrams
Two-Rate Policer
UDLR Tunnel ARP and IGMP Proxy
Uni-Directional Link Routing (UDLR)
Unicast Reverse Path Forwarding (uRPF)
User Maximum Links
Using 31-bit Prefixes on IPv4 Point-to-Point Links
V.110 support for Digital Modems
V.120 Support
V.92 Modem on Hold
Virtual Interface Template Service
Virtual Private Dial-up Network (VPDN)
Virtual Profile CEF Switched
Virtual Profiles
Virtual Router Redundancy Protocol (VRRP)
Virtual Templates for Protocol Translation
Voice Busyout Enhancements
Voice DSP Control Message Logger
Voice over ATM
Voice over ATM with AAL2 Trunking
Voice over Frame Relay (FRF.11)
Voice over Frame Relay Configuration Updates
Voice Over IP
Voice over IP Q.SIG Network Transparency
VoIP and Cisco Express Forwarding (CEF) Interoperability
VoIP and Policy Based Routing (PBR) Interoperability
VoIP Authentication (UNI-OSP)
VoIP Call Admission Control using RSVP
VoIP Gateway Trunk and Carrier Based Routing Enhancements
VPDN Group Session Limiting
VPN Tunnel Management
WCCP Redirection on Inbound Interfaces
WCCP Version 1
WCCP Version 2
Weighted Fair Queueing (WFQ)
Weighted RED (WRED)
Wildcard Pre-Shared Key
WRED Enhancement - Explicit Congestion Notification (ECN)
x Digital Subscriber Line (xDSL) Bridge Support
X.25
X.25 Annex G Session Status Change Reporting
X.25 Calling Address Insertion and Removal Based on Input Interface
X.25 Closed User Group
X.25 Failover
X.25 Load Balancing
X.25 on ISDN D-Channel
X.25 over Frame Relay (Annex G)
X.25 over TCP (XOT)
X.25 Over TCP Profiles
X.25 Remote Failure Detection
X.25 Switch Local Acknowledgement
X.25 Switching between PVCs and SVCs
X.28 Emulation

7563
3

To find out more about your selected release, you can use the Bug Toolkit

Close Window

AP GI

Cisco IOS File System Commands

This chapter describes the basic set of commands used to manipulate files on your routing device using the Cisco IOS File System (IFS) in Cisco IOS Release 12.2.

Commands in this chapter use URLs as part of the command syntax. URLs used in the Cisco IFS contain two parts: a file system or network prefix, and a file identification suffix. The following tables list URL keywords that can be used in the *source-url* and *destination-url* arguments for all commands in this chapter. The prefixes listed below can also be used in the *filesystem* arguments in this chapter.

Table 18 lists common URL network prefixes used to indicate a device on the network.

Table 18 Network Prefixes for Cisco IFS URLs

Prefix	Description
ftp:	Specifies a File Transfer Protocol (FTP) network server.
rcp:	Specifies an remote copy protocol (rcp) network server.
tftp:	Specifies a TFTP server.

Table 19 lists the available suffix options (file indentification suffixes) for the URL prefixes used in Table 18.

Table 19 File ID Suffixes for Cisco IFS URLs

Prefix	Suffix Options
ftp:	[[//[username[:password]@]location]/directory]/filename For example: **ftp://network-config** (*prefix://filename*) **ftp://jeanluc:secret@enterprise.cisco.com/ship-config**
rcp:	rcp:[[//[username@]location]/directory]/filename
tftp:	tftp:[[//location]/directory]/filename

Table 20 lists common URL prefixes used to indicate memory locations on the system.

First Published: April 30, 2001; Last Updated: July 31, 2002

Table 20 File System Prefixes for Cisco IFS URLs

Prefix	Description
bootflash:	Bootflash memory.
disk0:	Rotating disk media.
flash: [*partition-number*]	Flash memory. This prefix is available on most platforms. For platforms that do not have a device named **flash:**, the prefix **flash:** is aliased to **slot0:**. Therefore, you can use the prefix **flash:** to refer to the main Flash memory storage area on all platforms
flh:	Flash load helper log files.
null:	Null destination for copies. You can copy a remote file to null to determine its size.
nvram:	NVRAM. This is the default location for the running-configuration file.
slavebootflash:	Internal Flash memory on a slave RSP card of a router configured with Dual RSPs.
slavenvram:	NVRAM on a slave RSP card.
slaveslot0:	First PCMCIA card on a slave RSP card.
slaveslot1:	Second PCMCIA card on a slave RSP card.
slot0:	First PCMCIA Flash memory card.
slot1:	Second PCMCIA Flash memory card.
xmodem:	Obtain the file from a network machine using the Xmodem protocol.
ymodem:	Obtain the file from a network machine using the Ymodem protocol.

For details about the Cisco IFS, and for IFS configuration tasks, refer to the "Configuring the Cisco IOS File System" chapter in the Release 12.2 *Cisco IOS Configuration Fundamentals Configuration Guide*.

cd

To change the default directory or file system, use the **cd** EXEC command.

cd [*filesystem*:]

Syntax Description

filesystem:	(Optional) The URL or alias of the directory or file systems followed by a colon.

Defaults

The initial default file system is **flash:**. For platforms that do not have a physical device named **flash:**, the keyword **flash:** is aliased to the default Flash device.

If you do not specify a directory on a file system, the default is the root directory on that file system.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

For all EXEC commands that have an optional *filesystem* argument, the system uses the file system specified by the **cd** command when you omit the optional *filesystem* argument. For example, the **dir** EXEC command, which displays a list of files on a file system, contain an optional *filesystem* argument. When you omit this argument, the system lists the files on the file system specified by the **cd** command.

Examples

In the following example, the cd command is used to set the default file system to the Flash memory card inserted in slot 0:

```
Router# pwd
bootflash:/
Router# cd slot0:
Router# pwd
slot0:/
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the **cd** command.
show file systems	Lists available file systems and their alias prefix names.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

7559 w

configure network

The **configure network** command was replaced by the **copy** {**rcp** | **tftp**} **running-config** command in Cisco IOS Release 11.0. To maintain backward compatibility, the **configure network** command continues to function in Cisco IOS Release 12.2 for most systems, but support for this command may be removed in a future release.

The **copy** {**rcp** | **tftp**} **running-config** command was replaced by the **copy** {**ftp:** | **rcp:** | **tftp:**}[*filename*] **system:running-config** command in Cisco IOS Release 12.1.

The **copy** {**ftp:** | **rcp:** | **tftp:**}[*filename*] **system:running-config** command specifies that a configuration file should be copied from a FTP, rcp, or TFTP source to the running configuration. See the description of the **copy** in this chapter command for more information.

copy

To copy any file from a source to a destination, use the **copy** EXEC command.

copy [**/erase**] *source-url destination-url*

Syntax Description

/erase	(Optional) Erases the destination file system before copying.
source-url	The location URL or alias of the source file or directory to be copied.
destination-url	The destination URL or alias of the copied file or directory.

The exact format of the source and destination URLs varies according to the file or directory location. You may enter either an alias keyword for a particular file or an alias keyword for a file system type (not a file within a type).

Timesaver Aliases are used to cut down on the amount of typing you need to perform. For example, it is easier to type **copy run start** (the abbreviated form of the **copy running-config startup-config** command) than it is to type **copy system:r nvram:s** (the abbreviated form of the **copy system:running-config nvram:startup-config** command). These aliases also allow you to continue using some of the common commands used in previous versions of Cisco IOS software.

Table 21 shows two keyword shortcuts to URLs.

Table 21 Common Keyword Aliases to URLs

Keyword	Source or Destination
running-config	(Optional) Keyword alias for the **system:running-config** URL. The **system:running-config** keyword represents the current running configuration file. This keyword does not work in **more** and **show file** EXEC command syntaxes.
startup-config	(Optional) Keyword alias for the **nvram:startup-config** URL. The **nvram:startup-config** keyword represents the configuration file used during initialization (startup). This file is contained in NVRAM for all platforms except the Cisco 7000 family, which uses the CONFIG_FILE environment variable to specify the startup configuration. The Cisco 4500 series cannot use the **copy running-config startup-config** command. This keyword does not work in **more** and **show file** EXEC command syntaxes.

The following tables list aliases by file system type. If you do not specify an alias, the router looks for a file in the current directory.

Table 22 lists URL aliases for Special (opaque) file systems. Table 23 lists them for network file systems, and Table 24 lists them for local writable storage.

Table 22 URL Prefix Aliases for Special File Systems

Alias	Source or Destination
flh:	Source URL for flash load helper log files.
modem:	Destination URL for loading modem firmware on Cisco 5200 and 5300 Series routers.
nvram:	Router NVRAM. You can copy the startup configuration into or from NVRAM. You can also display the size of a private configuration file.
null:	Null destination for copies or files. You can copy a remote file to null to determine its size.
system:	Source or destination URL for system memory, which includes the running configuration.
xmodem:	Source destination for the file from a network machine that uses the Xmodem protocol.
ymodem:	Source destination for the file from a network machine that uses th Xmodem protocol.

Table 23 URL Prefix Aliases for Network File Systems

Alias	Source or Destination
ftp:	Source or destination URL for an File Transfer Protocol (FTP) network server. The syntax for this alias is as follows: **ftp:**[[[//*username* [:*password*]@]*location*]/*directory*]/*filename*.
rcp:	Source or destination URL for a Remote Copy Protocol (rcp) network server. The syntax for this alias is as follows: **rcp:**[[[//*username*@]*location*]/*directory*]/*filename*.
tftp:	Source or destination URL for a TFTP network server. The syntax for this alias is **tftp:**[[//*location*]/*directory*]/*filename*.

Table 24 URL Prefix Aliases for Local Writable Storage File Systems

Alias	Source or Destination
bootflash:	Source or destination URL for boot flash memory.
disk0: and disk1:	Source or destination URL of rotating media.
flash:	Source or destination URL for Flash memory. This alias is available on all platforms. For platforms that lack a flash: device, note that **flash:** is aliased to **slot0:**, allowing you to refer to the main Flash memory storage area on all platforms.
slavebootflash:	Source or destination URL for internal Flash memory on the slave RSP card of a router configured for HSA.
slaveram:	NVRAM on a slave RSP card of a router configured for HSA.
slaveslot0:	Source or destination URL of the first PCMCIA card on a slave RSP card of a router configured for HSA.

Table 24 URL Prefix Aliases for Local Writable Storage File Systems (continued)

Alias	Source or Destination
slaveslot1:	Source or destination URL of the second PCMCIA slot on a slave RSP card of a router configured for HSA.
slot0:	Source or destination URL of the first PCMCIA Flash memory card.
slot1:	Source or destination URL of the second PCMCIA Flash memory card.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

You can enter on the command line all necessary source- and destination-URL information and the username and password to use, or you can enter the **copy** command and have the router prompt you for any missing information.

If you enter information, choose one of the following three options: **running-config**, **startup-config**, or a file system alias (see previous tables.) The location of a file system dictates the format of the source or destination URL.

The colon is required after the alias. However, earlier commands not requiring a colon remain supported, but are unavailable in context-sensitive help.

The entire copying process may take several minutes and differs from protocol to protocol and from network to network.

In the alias syntax for **ftp:**, **rcp:**, and **tftp:**, the location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers.

This section contains usage guidelines for the following topics:

- Understanding Invalid Combinations of Source and Destination
- Understanding Character Descriptions
- Understanding Partitions
- Using rcp
- Using FTP
- Storing Images on Servers
- Copying from a Server to Flash Memory
- Verifying Images
- Copying a Configuration File from a Server to the Running Configuration
- Copying a Configuration File from a Server to the Startup Configuration
- Storing the Running or Startup Configuration on a Server
- Saving the Running Configuration to the Startup Configuration

- Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables
- Using the Copy Command with the Dual RSP Feature

Understanding Invalid Combinations of Source and Destination

Some invalid combinations of source and destination exist. Specifically, you cannot copy the following:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

Understanding Character Descriptions

Table 25 describes the characters that you may see during processing of the **copy** command.

Table 25 copy Character Descriptions

Character	Description
!	For network transfers, an exclamation point indicates that the copy process is taking place. Each exclamation point indicates the successful transfer of ten packets (512 bytes each).
.	For network transfers, a period indicates that the copy process timed out. Many periods in a row typically mean that the copy process may fail.
O	For network transfers, an uppercase O indicates that a packet was received out of order and the copy process may fail.
e	For Flash erasures, a lowercase e indicates that a device is being erased.
E	An uppercase E indicates an error. The copy process may fail.
V	A series of uppercase Vs indicates the progress during the verification of the image checksum.

Understanding Partitions

You cannot copy an image or configuration file to a Flash partition from which you are currently running. For example, if partition 1 is running the current system image, copy the configuration file or image to partition 2. Otherwise, the copy operation will fail.

You can identify the available Flash partitions by entering the **show file system** EXEC command.

Using rcp

The rcp protocol requires a client to send a remote username upon each rcp request to a server. When you copy a configuration file or image between the router and a server using rcp, the Cisco IOS software sends the first valid username it encounters in the following sequence:

1. The remote username specified in the **copy** command, if a username is specified.
2. The username set by the **ip rcmd remote-username** global configuration command, if the command is configured.
3. The remote username associated with the current tty (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the router software sends the Telnet username as the remote username.
4. The router host name.

For the rcp copy request to process, an account must be defined on the network server for the remote username. If the network administrator of the destination server did not establish an account for the remote username, this command will not run. If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the remote username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

If you are writing to the server, the rcp server must be properly configured to accept the rcp write request from the user on the router. For UNIX systems, add an entry to the .rhosts file for the remote user on the rcp server. Suppose the router contains the following configuration lines:

```
hostname Rtr1
ip rcmd remote-username User0
```

If the router IP address translates to Router1.company.com, then the .rhosts file for User0 on the rcp server should contain the following line:

```
Router1.company.com Rtr1
```

Refer to the documentation for your rcp server for more details.

If you are using a personal computer as a file server, the computer must support the remote shell protocol (rsh).

Using FTP

The FTP protocol requires a client to send a remote username and password upon each FTP request to a server. When you copy a configuration file from the router to a server using FTP, the Cisco IOS software sends the first valid username that it encounters in the following sequence:

1. The username specified in the **copy** command, if a username is specified.
2. The username set by the **ip ftp username** command, if the command is configured.
3. Anonymous.

The router sends the first valid password in the following list:

1. The password specified in the **copy** command, if a password is specified.
2. The password set by the **ip ftp password** command, if the command is configured.
3. The router forms a password username@routername.domain. The variable username is the username associated with the current session, routername is the configured host name, and domain is the domain of the router.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user on the router.

If the server has a directory structure, the configuration file or image is written to or copied from the directory associated with the username on the server. For example, if the system image resides in the home directory of a user on the server, specify that user name as the remote username.

Refer to the documentation for your FTP server for more details.

Use the **ip ftp username** and **ip ftp password** global configuration commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify a username for that copy operation only.

Storing Images on Servers

Use the **copy** *flash: destination-url* command (for example, **copy flash: tftp:**) to copy a system image or boot image from Flash memory to a network server. Use the copy of the image as a backup copy. Also, use it to verify that the copy in Flash memory is the same as that in the original file.

Copying from a Server to Flash Memory

Use the **copy** *destination-url flash:* command (for example, **copy tftp: flash:**) to copy an image from a server to Flash memory.

On Class B file system platforms, the system provides an option to erase existing Flash memory before writing onto it.

Note Verify the image in Flash memory before booting the image.

Verifying Images

When copying a new image to your router, you should confirm that the image was not corrupted during the copy process. Depending on the destination filesystem type, a checksum for the image file may be displayed when the **copy** command completes. You can verify this checksum by comparing it to the checksum value provided for your image file on Cisco.com.

Caution If the checksum values do not match, do not reboot the router. Instead, reissue the **copy** command and compare the checksums again. If the checksum is repeatedly wrong, copy the original image back into Flash memory *before* you reboot the router from Flash memory. If you have a corrupted image in Flash memory and try to boot from Flash memory, the router will start the system image contained in ROM (assuming booting from a network server is not configured). If ROM does not contain a fully functional system image, the router might not function and will need to be reconfigured through a direct console port connection.

An alternate method for file verification is to use the UNIX 'diff' command. This method can also be applied to file types other than Cisco IOS images. If you suspect that a file is corrupted, copy the suspect file and the original file to a Unix server. (The file names may need to be modified if you try to save the files in the same directory.) Then run the Unix 'diff' command on the two files. If there is no difference, then the file has not been corrupted.

Copying a Configuration File from a Server to the Running Configuration

Use the **copy** {**ftp:** | **rcp:** | **tftp:**} **running-config** command to load a configuration file from a network server to the running configuration of the router (note that **running-config** is the alias for the **system:running-config** keyword). The configuration will be added to the running configuration as if the commands were typed in the command-line interface (CLI). Thus, the resulting configuration file will be a combination of the previous running configuration and the loaded configuration file, with the loaded configuration file having precedence.

You can copy either a host configuration file or a network configuration file. Accept the default value of *host* to copy and load a host configuration file containing commands that apply to one network server in particular. Enter *network* to copy and load a network configuration file containing commands that apply to all network servers on a network.

Copying a Configuration File from a Server to the Startup Configuration

Use the **copy** {**ftp:** | **rcp:** | **tftp:**} **nvram:startup-config** command to copy a configuration file from a network server to the router startup configuration. These commands replace the startup configuration file with the copied configuration file.

Storing the Running or Startup Configuration on a Server

Use the **copy system:running-config** {**ftp:** | **rcp:** | **tftp:**} command to copy the current configuration file to a network server using FTP, rcp, or TFTP. Use the **copy nvram:startup-config** {**ftp:** | **rcp:** | **tftp:**} command to copy the startup configuration file to a network server.

The configuration file copy can serve as a backup copy.

Saving the Running Configuration to the Startup Configuration

Use the **copy system:running-config nvram:startup-config** command to copy the running configuration to the startup configuration.

Note Some specific commands might not get saved to NVRAM. You will need to enter these commands again if you reboot the machine. These commands are noted in the documentation. We recommend that you keep a listing of these settings so you can quickly reconfigure your router after rebooting.

If you issue the **copy system:running-config nvram:startup-config** command from a bootstrap system image, a warning will instruct you to indicate whether you want your previous NVRAM configuration to be overwritten and configuration commands to be lost. This warning does not appear if NVRAM contains an invalid configuration or if the previous configuration in NVRAM was generated by a bootstrap system image.

On all platforms except Class A file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to NVRAM.

On the Class A Flash file system platforms, the **copy system:running-config nvram:startup-config** command copies the currently running configuration to the location specified by the CONFIG_FILE environment variable. This variable specifies the device and configuration file used for initialization. When the CONFIG_FILE environment variable points to NVRAM or when this variable does not exist (such as at first-time startup), the software writes the current configuration to NVRAM. If the current configuration is too large for NVRAM, the software displays a message and stops executing the command.

When the CONFIG_FILE environment variable specifies a valid device other than **nvram:** (that is, **flash:**, **bootflash:**, **slot0:**, or **slot1:**), the software writes the current configuration to the specified device and filename, and stores a distilled version of the configuration in NVRAM. A distilled version is one that does not contain access list information. If NVRAM already contains a copy of a complete configuration, the router prompts you to confirm the copy.

Using CONFIG_FILE, BOOT, and BOOTLDR Environment Variables

For the Class A Flash file system platforms, specifications are as follows:

- The CONFIG_FILE environment variable specifies the configuration file used during router initialization.
- The BOOT environment variable specifies a list of bootable images on various devices.
- The BOOT environment variable specifies a list of bootable images on various devices.
- The BOOTLDR environment variable specifies the Flash device and filename containing the rxboot image that ROM uses for booting.

4556

- Cisco 3600 routers do not use a dedicated boot helper image (rxboot), which many other routers use to help with the boot process. Instead, the BOOTLDR ROM monitor environment variable identifies the Flash memory device and filename that are used as the boot helper; the default is the first system image in Flash memory.

To view the contents of environment variables, use the **show bootvar** EXEC command. To modify the CONFIG_FILE environment variable, use the **boot config** global configuration command. To modify the BOOTLDR environment variable, use the **boot bootldr** global configuration command. To modify the BOOT environment variable, use the **boot system** global configuration command. To save your modifications, use the **copy system:running-config nvram:startup-config** command.

When the destination of a **copy** command is specified by the CONFIG_FILE or BOOTLDR environment variable, the router prompts you for confirmation before proceeding with the copy. When the destination is the only valid image in the BOOT environment variable, the router also prompts you for confirmation before proceeding with the copy.

Using the Copy Command with the Dual RSP Feature

The Dual RSP feature allows you to install two Route/Switch Processor (RSP) cards in a single router on the Cisco 7507 and Cisco 7513 platforms.

On a Cisco 7507 or Cisco 7513 router configured for Dual RSPs, if you copy a file to **nvram:startup-configuration** with automatic synchronization disabled, the system asks if you also want to copy the file to the slave startup configuration. The default answer is **yes**. If automatic synchronization is enabled, the system automatically copies the file to the slave startup configuration each time you use a **copy** command with **nvram:startup-configuration** as the destination.

Examples

The following examples illustrate uses of the **copy** command.

- Copying an Image from a Server to Flash Memory Examples
- Saving a Copy of an Image on a Server Examples
- Copying a Configuration File from a Server to the Running Configuration Example
- Copying a Configuration File from a Server to the Startup Configuration Example
- Copying the Running Configuration to a Server Example
- Copying the Startup Configuration to a Server Example
- Saving the Current Running Configuration Example
- Moving Configuration Files to Other Locations Examples
- Copying an Image from the Master RSP Card to the Slave RSP Card Example

Copying an Image from a Server to Flash Memory Examples

The following three examples use a **copy rcp:**, **copy tftp:**, or **copy ftp:** command to copy an image file from a server to Flash memory:

- Copying an Image from a Server to Flash Memory Example
- Copying an Image from a Server to a Flash Memory Using Flash Load Helper Example
- Copying an Image from a Server to a Flash Memory Card Partition Example

Copying an Image from a Server to Flash Memory Example

This example copies a system image named file1 from the remote rcp server with an IP address of 172.16.101.101 to Flash memory. On Class B file system platforms, the Cisco IOS software allows you to first erase the contents of Flash memory to ensure that enough Flash memory is available to accommodate the system image.

```
Router# copy rcp://netadmin@172.16.101.101/file1 flash:file1

Destination file name [file1]?
Accessing file 'file1' on 172.16.101.101...
Loading file1 from 172.16.101.101 (via Ethernet0): ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'file1' from server
  as 'file1' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee...erased
Loading file1 from 172.16.101.101 (via Ethernet0): !
[OK - 984/8388608 bytes]

Verifying checksum... OK (0x14B3)
Flash copy took 0:00:01 [hh:mm:ss]
```

Copying an Image from a Server to a Flash Memory Using Flash Load Helper Example

The following example copies a system image into a partition of Flash memory. The system will prompt for a partition number only if there are two or more read/write partitions or one read-only and one read/write partition and dual Flash bank support in boot ROMs. If the partition entered is not valid, the process terminates. You can enter a partition number, a question mark (?) for a directory display of all partitions, or a question mark and a number (?*number*) for directory display of a particular partition. The default is the first read/write partition. In this case, the partition is read-only and has dual Flash bank support in boot ROM, so the system uses Flash Load Helper.

```
Router# copy tftp: flash:

System flash partition information:
Partition   Size    Used    Free    Bank-Size   State        Copy-Mode
    1       4096K   2048K   2048K   2048K       Read Only    RXBOOT-FLH
    2       4096K   2048K   2048K   2048K       Read/Write   Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]

                              **** NOTICE ****
Flash load helper v1.0
This process will accept the copy options and then terminate
the current system image to use the ROM based image for the copy.
Routing functionality will not be available during that time.
If you are logged in via telnet, this connection will terminate.
Users with console access can see the results of the copy operation.
                              ---- ******** ----
Proceed? [confirm]
System flash directory, partition 1:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [255.255.255.255]? 172.16.1.1
Source file name? master/igs-bfpx-100.4.3
Destination file name [default = source name]?

Loading master/igs-bfpx.100-4.3 from 172.16.1.111: !
```

```
Erase flash device before writing? [confirm]
Flash contains files. Are you sure? [confirm]
Copy 'master/igs-bfpx.100-4.3' from TFTP server
as 'master/igs-bfpx.100-4.3' into Flash WITH erase? [yes/no] yes
```

Copying an Image from a Server to a Flash Memory Card Partition Example

The following example copies the file c3600-i-mz from the rcp server at IP address 172.23.1.129 to the Flash memory card in slot 0 of a Cisco 3600 series router, which has only one partition. As the operation progresses, the Cisco IOS software asks you to erase the files on the Flash memory PC card to accommodate the incoming file. This entire operation takes 18 seconds to perform, as indicated at the end of the example.

```
Router# copy rcp: slot0:

PCMCIA Slot0 flash

Partition    Size     Used      Free      Bank-Size  State          Copy Mode
  1          4096K    3068K     1027K     4096K      Read/Write     Direct
  2          4096K    1671K     2424K     4096K      Read/Write     Direct
  3          4096K       0K     4095K     4096K      Read/Write     Direct
  4          4096K    3825K      270K     4096K      Read/Write     Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]

PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   3142288  c3600-j-mz.test
[3142352 bytes used, 1051952 available, 4194304 total]
Address or name of remote host [172.23.1.129]?
Source file name? /tftpboot/images/c3600-i-mz
Destination file name [/tftpboot/images/c3600-i-mz]?
Accessing file '/tftpboot/images/c3600-i-mz' on 172.23.1.129...
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz: ! [OK]

Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy '/tftpboot/images/c3600-i-mz' from server
  as '/tftpboot/images/c3600-i-mz' into Flash WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Connected to 172.23.1.129
Loading 1711088 byte file c3600-i-mz:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying checksum...  OK (0xF89A)
Flash device copy took 00:00:18 [hh:mm:ss]
```

Saving a Copy of an Image on a Server Examples

The following four examples use **copy** commands to copy image files to a server for storage:

- Copy an Image from Flash Memory to an rcp Server Example
- Copy an Image from a Partition of Flash Memory to a Server Example
- Copying an Image from a Flash Memory File System to an FTP Server Example
- Copying an Image from Boot Flash Memory to a TFTP Server Example

Copy an Image from Flash Memory to an rcp Server Example

The following example copies a system image from Flash Memory to an rcp server using the default remote username. Because the rcp server address and filename are not included in the command, the router prompts for it.

```
Router# copy flash: rcp:

IP address of remote host [255.255.255.255]? 172.16.13.110
Name of file to copy? gsxx
writing gsxx - copy complete
```

Copy an Image from a Partition of Flash Memory to a Server Example

The following example copies an image from a particular partition of Flash memory to an rcp server using a remote username of netadmin1.

The system will prompt if there are two or more partitions. If the partition entered is not valid, the process terminates. You have the option to enter a partition number, a question mark (?) for a directory display of all partitions, or a question mark and a number (?*number*) for a directory display of a particular partition. The default is the first partition.

```
Router# configure terminal
Router# ip rcmd remote-username netadmin1
Router# end
Router# copy flash: rcp:
System flash partition information:
Partition    Size     Used     Free     Bank-Size     State          Copy-Mode
    1        4096K    2048K    2048K    2048K         Read Only      RXBOOT-FLH
    2        4096K    2048K    2048K    2048K         Read/Write     Direct
[Type ?<number> for partition directory; ? for full directory; q to abort]
Which partition? [1] 2

System flash directory, partition 2:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]
Address or name of remote host [ABC.CISCO.COM]?
Source file name? master/igs-bfpx.100-4.3
Destination file name [master/igs-bfpx.100-4.3]?
Verifying checksum for 'master/igs-bfpx.100-4.3' (file # 1)... OK
Copy 'master/igs-bfpx.100-4.3' from Flash to server
as 'master/igs-bfpx.100-4.3'? [yes/no] yes
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Copying an Image from a Flash Memory File System to an FTP Server Example

The following example copies the file c3600-i-mz from partition 1 of the Flash memory card in slot 0 to an FTP server at IP address 172.23.1.129.

```
Router# show slot0: partition 1

PCMCIA Slot0 flash directory, partition 1:
File  Length   Name/status
  1   1711088 c3600-i-mz
[1711152 bytes used, 2483152 available, 4194304 total]

Router# copy slot0:1:c3600-i-mz ftp://myuser:mypass@172.23.1.129/c3600-i-mz
Verifying checksum for '/tftpboot/cisco_rules/c3600-i-mz' (file # 1)...  OK
Copy '/tftpboot/cisco_rules/c3600-i-mz' from Flash to server
  as 'c3700-i-mz'? [yes/no] yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upload to server done
Flash device copy took 00:00:23 [hh:mm:ss]
```

4547 3

Copying an Image from Boot Flash Memory to a TFTP Server Example

The following example copies an image from boot Flash memory to a TFTP server:

```
Router# copy bootflash:file1 tftp://192.168.117.23/file1

Verifying checksum for 'file1' (file # 1)... OK
Copy 'file1' from Flash to server
  as 'file1'? [yes/no]y
!!!!...
Upload to server done
Flash copy took 0:00:00 [hh:mm:ss]
```

Copying a Configuration File from a Server to the Running Configuration Example

The following example copies and runs a configuration filename host1-confg from the netadmin1 directory on the remote server with an IP address of 172.16.101.101:

```
Router# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config

Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
Router#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

Copying a Configuration File from a Server to the Startup Configuration Example

The following example copies a configuration file host2-confg from a remote FTP server to the startup configuration. The IP address is172.16.101.101, the remote username is netadmin1, and the remote password is ftppass.

```
Router# copy ftp://netadmin1:ftppass@172.16.101.101/host2-confg nvram:startup-config
Configure using rtr2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file rtr2-confg:![OK]
[OK]
Router#
%SYS-5-CONFIG_NV:Non-volatile store configured from rtr2-config by
FTP from 172.16.101.101
```

Copying the Running Configuration to a Server Example

The following example specifies a remote username of netadmin1. Then it copies the running configuration file named rtr2-confg to the netadmin1 directory on the remote host with an IP address of 172.16.101.101.

```
Router# configure terminal
Router(config)# ip rcmd remote-username netadmin1
Router(config)# end
Router# copy system:running-config rcp:
Remote host[]? 172.16.101.101

Name of configuration file to write [Rtr2-confg]?
Write file rtr2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
```

Copying the Startup Configuration to a Server Example

The following example copies the startup configuration to a TFTP server:

```
Router# copy nvram:startup-config tftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [rtr2-confg]? <cr>
Write file rtr2-confg on host 172.16.101.101?[confirm] <cr>
![OK]
```

Saving the Current Running Configuration Example

The following example copies the running configuration to the startup configuration. On a Class A Flash file system platform, this command copies the running configuration to the startup configuration specified by the CONFIG_FILE variable.

```
copy system:running-config nvram:startup-config
```

The following example shows the warning that the system provides if you try to save configuration information from bootstrap into the system:

```
Router(boot)# copy system:running-config nvram:startup-config

Warning: Attempting to overwrite an NVRAM configuration written
by a full system image. This bootstrap software does not support
the full configuration command set. If you perform this command now,
some configuration commands may be lost.
Overwrite the previous NVRAM configuration?[confirm]
```

Enter **no** to escape writing the configuration information to memory.

Moving Configuration Files to Other Locations Examples

On some routers, you can store copies of configuration files on a Flash memory device. Five examples follow.

Copying the Startup Configuration to a Flash Memory Device Example

The following example copies the startup configuration file (specified by the CONFIG_FILE environment variable) to a Flash memory card inserted in slot 0:

```
copy nvram:startup-config slot0:router-confg
```

Copying the Running Configuration to a Flash Memory Device Example

The following example copies the running configuration from the router to the Flash memory PC card in slot 0:

```
Router# copy system:running-config slot0:berlin-cfg

Building configuration...
```

```
5267 bytes copied in 0.720 secs
```

4545
W

Copying to the Running Configuration from a Flash Memory Device Example

The following example copies the file named ios-upgrade-1 from the Flash memory card in slot 0 to the running configuration:

```
Router# copy slot0:4:ios-upgrade-1 system:running-config

Copy 'ios-upgrade-1' from flash device
  as 'running-config' ? [yes/no] yes
```

Copying to the Startup Configuration from a Flash Memory Device Example

The following example copies the router-image file from the Flash memory to the startup configuration:

```
copy flash:router-image nvram:startup-config
```

Copying a Configuration File from one Flash Device to Another Example

The following example copies the file running-config from the first partition in internal Flash memory to the Flash memory PC card in slot 1. The checksum of the file is verified, and its copying time of 30 seconds is displayed.

```
Router# copy flash: slot1:

System flash

Partition    Size     Used      Free      Bank-Size  State          Copy Mode
  1          4096K    3070K     1025K     4096K      Read/Write     Direct
  2         16384K    1671K    14712K     8192K      Read/Write     Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 1]

System flash directory, partition 1:
File  Length   Name/status
  1   3142748  dirt/images/mars-test/c3600-j-mz.latest
  2   850      running-config
[3143728 bytes used, 1050576 available, 4194304 total]

PCMCIA Slot1 flash directory:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
  2   850      running-config
[1712068 bytes used, 2482236 available, 4194304 total]
Source file name? running-config
Destination file name [running-config]?
Verifying checksum for 'running-config' (file # 2)...  OK
Erase flash device before writing? [confirm]
Flash contains files. Are you sure you want to erase? [confirm]

Copy 'running-config' from flash: device
  as 'running-config' into slot1: device WITH erase? [yes/no] yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
!
 [OK - 850/4194304 bytes]

Flash device copy took 00:00:30 [hh:mm:ss]
Verifying checksum...  OK (0x16)
```

Copying an Image from the Master RSP Card to the Slave RSP Card Example

The following example copies the router-image file from the Flash memory card inserted in slot 1 of the master RSP card to slot 0 of the slave RSP card in the same router:

```
copy slot1:router-image slaveslot0:
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
boot system	Specifies the system image that the router loads at startup.
cd	Changes the default directory or file system.
copy xmodem: flash:	Copies any file from a source to a destination.
copy ymodem: flash:	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
erase	Erases a file system.
ip rcmd remote-username	Configures the remote username to be used when requesting a remote copy using rcp.
reload	Reloads the operating system.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
show (Flash file system)	Displays the layout and contents of a Flash memory file system.
slave auto-sync config	Turns on automatic synchronization of configuration files for a Cisco 7507 or Cisco 7513 router that is configured for Dual RSP Backup.
verify bootflash:	Either of the identical **verify bootflash:** or **verify bootflash** commands replaces the **copy verify bootflash** command. Refer to the **verify** command for more information.

delete

To delete a file from a Flash memory device or NVRAM, use the **delete** EXEC command.

delete *URL* [**/force** | **/recursive**]

Syntax Description

URL	IFS URL of the file to be deleted. Include the filesystem prefix, followed by a colon, and, optionally, the name of a file or directory.
/force	(Optional) Deletes the specified file or directory with prompting you for verification. **Note** Use this keyword with caution: the system will not ask you to confirm the file deletion.
/recursive	(Optional) Deletes all files in the specified directory, as well as the directory itself.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

If you attempt to delete the configuration file or image specified by the CONFIG_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion.

When you delete a file in Flash memory, the software simply marks the file as deleted, but it does not erase the file. To later recover a "deleted" file in Flash memory, use the **undelete** EXEC command. You can delete and undelete a file up to 15 times.

To permanently delete all files marked "deleted" on a linear Flash memory device, use the **squeeze** EXEC command.

Examples

The following example deletes the file named "test" from the Flash filesystem:

```
Router# delete flash:test
Delete flash:test? [confirm]
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.

Command	Description
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

7541
3

dir

To display a list of files on a file system, use the **dir** EXEC command.

dir [**/all**] [*filesystem*:][*file-url*]

Syntax Description

/all	(Optional) Lists deleted files, undeleted files, and files with errors.
filesystem:	(Optional) File system or directory containing the files to list, followed by a colon.
file-url	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Defaults

The default file system is specified by the **cd** command. When you omit the **/all** keyword, the Cisco I software displays only undeleted files.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use the **show** (Flash file system) command to display more detail about the files in a particular file system.

Examples

The following is sample output from the **dir** command:

```
Router# dir slot0:

Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  5  -rw-         639   Oct 02 1997 12:09:32 rally
  7  -rw-         639   Oct 02 1997 12:37:13  the_time

20578304 bytes total (3104544 bytes free)

Router# dir /all slot0:

Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  3  -rw-     7982828   Oct 01 1997 18:48:14  [rsp-jsv-mz]
  4  -rw-         639   Oct 02 1997 12:09:17  [the_time]
```

```
 5  -rw-         639   Oct 02 1997 12:09:32  rally
 6  -rw-         639   Oct 02 1997 12:37:01  [the_time]
 7  -rw-         639   Oct 02 1997 12:37:13  the_time
```

Table 26 describes the significant fields shown in the displays.

Table 26 dir Field Descriptions

Field	Description
1	Index number of the file.
-rw-	Permissions. The file can be any or all of the following: • d—directory • r—readable • w—writable • x—executable
4720148	Size of the file.
Aug 29 1997 17:49:36	Last modification date.
hampton/nitro/c7200-j-mz	Filename. Deleted files are indicated by square brackets around the filename.

Related Commands

Command	Description
cd	Changes the default directory or file system.
delete	Deletes a file on a Flash memory device.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

erase

To erase a file system, use the **erase** EXEC command. The **erase nvram:** command replaces the **write erase** command and the **erase startup-config** command.

erase *filesystem*:

Syntax Description

filesystem:	File system name, followed by a colon. For example, **flash:** or **nvram:**

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

When a file system is erased, none of the files in the file system can be recovered.

The **erase** command can be used on both Class B and Class C Flash file systems only. To reclaim space on Flash file systems after deleting files using the **delete** command, you must use the **erase** command. This command erases all of the files in the Flash file system.

Class A Flash file systems cannot be erased. You can delete individual files using the **delete** EXEC command and then reclaim the space using the **squeeze** EXEC command. You can use the **format** EXEC command to format the Flash file system.

On Class C Flash file systems, space is dynamically reclaimed when you use the **delete** command. You can also use either the **format** or **erase** command to reinitialize a Class C Flash file system.

The **erase nvram:** command erases NVRAM. On Class A file system platforms, if the CONFIG_FILE variable specifies a file in Flash memory, the specified file will be marked "deleted."

Examples

The following example erases the NVRAM, including the startup configuration located there:

```
erase nvram:
```

The following example erases all of partition 2 in internal Flash memory:

```
Router# erase flash:2

System flash directory, partition 2:
File  Length   Name/status
  1   1711088  dirt/images/c3600-i-mz
[1711152 bytes used, 15066064 available, 16777216 total]

Erase flash device, partition 2? [confirm]
Are you sure? [yes/no]: yes
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
```

The following example erases Flash memory when Flash is partitioned, but no partition is specified in the command:

```
Router# erase flash:

System flash partition information:
Partition    Size     Used     Free     Bank-Size    State          Copy-Mode
     1       4096K    2048K    2048K    2048K        Read Only      RXBOOT-FLH
     2       4096K    2048K    2048K    2048K        Read/Write     Direct

[Type ?<no> for partition directory; ? for full directory; q to abort]
Which partition? [default = 2]
```

The system will prompt only if there are two or more read/write partitions. If the partition entered is not valid or is the read-only partition, the process terminates. You can enter a partition number, a question mark (**?**) for a directory display of all partitions, or a question mark and a number (**?***number*) for directory display of a particular partition. The default is the first read/write partition.

```
System flash directory, partition 2:
File  Length   Name/status
  1   3459720  master/igs-bfpx.100-4.3
[3459784 bytes used, 734520 available, 4194304 total]

Erase flash device, partition 2? [confirm] <Return>
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
delete	Deletes a file on a Flash memory device.
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

erase bootflash

The **erase bootflash:** and **erase bootflash** commands have identical functions. See the description of the **erase** command in this chapter for more information.

file prompt

To specify the level of prompting, use the **file prompt** global configuration command.

file prompt [alert | noisy | quiet]

Syntax Description

alert	(Optional) Prompts only for destructive file operations. This is the default.
noisy	(Optional) Confirms all file operation parameters.
quiet	(Optional) Seldom prompts for file operations.

Defaults

alert

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to change the amount of confirmation needed for different file operations.

This command affects only prompts for confirmation of operations. The router will always prompt for missing information.

Examples

The following example configures confirmation prompting for all file operations:

```
file prompt noisy
```

7535 3

format

To format a Class A or Class C Flash file system, use the **format** EXEC command.

Class C Flash File System

format *filesystem1*:

Class A Flash File System

format [**spare** *spare-number*] *filesystem1*: [[*filesystem2*:][*monlib-filename*]]

Caution Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the Flash memory card can still be used. Otherwise, you must reformat the Flash card when some of the sectors fail.

Syntax Description

spare	(Optional) Reserves spare sectors as specified by the *spare-number* argument when formatting Flash memory.
spare-number	(Optional) Number of the spare sectors to reserve on formatted Flash memory. Valid values are from 0 to 16. The default value is zero.
filesystem1:	Flash memory to format, followed by a colon.
filesystem2:	(Optional) File system containing the monlib file to use for formatting filesystem1 followed by a colon.
monlib-filename	(Optional) Name of the ROM monitor library file (monlib file) to use for formatting the *filesystem1* argument. The default monlib file is the one bundled with the system software. When used with HSA and you do not specify the *monlib-filename* argument, the system takes ROM monitor library file from the slave image bundle. If you specify the *monlib-filename* argument, the system assumes that the files reside on the slave devices.

Defaults

The default monlib file is the one bundled with the system software.

The default number of spare sectors is zero (0).

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use this command to format Class A or C Flash memory file systems.

In some cases, you might need to insert a new PCMCIA Flash memory card and load images or backup configuration files onto it. Before you can use a new Flash memory card, you must format it.

Sectors in Flash memory cards can fail. Reserve certain Flash memory sectors as "spares" by using the optional *spare* argument on the **format** command to specify 0 to 16 sectors as spares. If you reserve a small number of spare sectors for emergencies, you can still use most of the Flash memory card. If you specify 0 spare sectors and some sectors fail, you must reformat the Flash memory card, thereby erasing all existing data.

The monlib file is the ROM monitor library. The ROM monitor uses this file to access files in the Flash file system. The Cisco IOS system software contains a monlib file.

In the command syntax, *filesystem1:* specifies the device to format and *filesystem2:* specifies the optional device containing the monlib file used to format *filesystem1:*. If you omit the optional *filesystem2:* and *monlib-filename* arguments, the system formats *filesystem1:* using the monlib file already bundled with the system software. If you omit only *the optional filesystem2:* argument, the system formats *filesystem1:* using the monlib file from the device you specified with the **cd** command. If you omit only the optional *monlib-filename* argument, the system formats *filesystem1:* using the *filesystem2:* monlib file. When you specify both arguments—*filesystem2:* and *monlib-filename*—the system formats *filesystem1:* using the monlib file from the specified device. You can specify *filesystem1:*'s own monlib file in this argument. If the system cannot find a monlib file, it terminates its formatting.

⚠ **Caution** You can read from or write to Flash memory cards formatted for Cisco 7000 series Route Processor (RP) cards in your Cisco 7200 and 7500 series routers, but you cannot boot the Cisco 7200 and 7500 series routers from a Flash memory card formatted for the Cisco 7000 series routers. Similarly, you can read from or write to Flash memory cards formatted for the Cisco 7200 and 7500 series routers in your Cisco 7000 series routers, but you cannot boot the Cisco 7000 series routers from a Flash memory card formatted for the Cisco 7200 and 7500 series routers.

Examples

The following example formats a Flash memory card inserted in slot 0:

```
Router# format slot0:

Running config file on this device, proceed? [confirm]y
All sectors will be erased, proceed? [confirm]y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device slot0 completed
```

When the console returns to the EXEC prompt, the new Flash memory card is formatted and ready for use.

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
delete	Deletes a file on a Flash memory device.
show file systems (Flash file system)	Lists available file systems.

Command	Description
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

fsck

To check a Class C Flash file system for damage and repair any problems, use the **fsck** EXEC command.

fsck [**/nocrc**] *filesystem*:

Syntax Description

/nocrc	(Optional) Omits cyclic redundancy checks (CRCs).
filesystem:	The file system to check.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is only valid on Class C Flash file systems.

Examples

The following example checks the Flash file system:

```
Router# fsck flash:

Fsck operation may take a while. Continue? [confirm]
flashfs[4]: 0 files, 2 directories
flashfs[4]: 0 orphaned files, 0 orphaned directories
flashfs[4]: Total bytes: 8128000
flashfs[4]: Bytes used: 1024
flashfs[4]: Bytes available: 8126976
flashfs[4]: flashfs fsck took 23 seconds.
Fsck of flash: complete
```

mkdir

To create a new directory in a Class C Flash file system, use the **mkdir** EXEC command.

mkdir *directory*

Syntax Description

directory	The name of the directory to create.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is only valid on Class C Flash file systems.

If you do not specify the directory name in the command line, the router prompts you for it.

Examples

The following example creates a directory named newdir:

```
Router# mkdir newdir

Mkdir file name [newdir]?
Created dir flash:newdir
Router# dir
Directory of flash:

  2  drwx           0   Mar 13 1993 13:16:21  newdir

8128000 bytes total (8126976 bytes free)
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
rmdir	Removes an existing directory in a Class C Flash file system.

more

To display a file, use the **more** EXEC command.

more [**/ascii** | **/binary** | **/ebcdic**] *file-url*

Syntax Description

/ascii	(Optional) Displays a binary file in ASCII format.
/binary	(Optional) Displays a file in hex/text format.
/ebcdic	(Optional) Displays a binary file in EBCDIC format.
file-url	The URL of the file to display.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

The **more system:running-config** command displays the same output as the **show running-config** command. The **more nvram:startup-config** command replaces the **show startup-config** command and the **show configuration** command.

You can use this command to display configuration files, as follows:

- The **more nvram:startup-config** command displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable. The Cisco IOS software informs you whether the displayed configuration is a complete configuration or a distilled version. A distilled configuration is one that does not contain access lists.
- The **more system:running-config** command displays the running configuration.

These commands show the version number of the software used when you last changed the configuration file.

You can display files on remote systems using the **more** command.

Examples

The following partial sample output displays the configuration file named startup-config in NVRAM:

```
Router# more nvram:startup-config

!
! No configuration change since last restart
! NVRAM config last updated at 02:03:26 PDT Thu Oct 2 1997
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service udp-small-servers
service tcp-small-servers
.
```

7529
3

```
.
.
end
```

The following is partial sample output from the **more nvram:startup-config** command when the configuration file has been compressed:

```
Router# more nvram:startup-config

Using 21542 out of 65536 bytes, uncompressed size = 142085 bytes
!
version 12.1
service compress-config
!
hostname rose
!
.
.
.
```

The following partial sample output displays the running configuration:

```
Router2# more system:running-config

Building configuration...

Current configuration:
!
version 12.1
no service udp-small-servers
no service tcp-small-servers
!
hostname Router2
!
.
.
.
!
end
```

Related Commands

Command	Description
boot config	Specifies the device and filename of the configuration file from which the router configures itself during initialization (startup).
service compress-config	Compresses startup configuration files.
show bootvar	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

pwd

To show the current setting of the **cd** command, use the **pwd** EXEC command.

pwd

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Use the **pwd** command to show which directory or file system is specified as the default by the **cd** command. For all EXEC commands that have an optional *filesystem* argument, the system uses the file system specified by the **cd** command when you omit the optional *filesystem* argument.

For example, the **dir** command contains an optional *filesystem* argument and displays a list of files on a particular file system. When you omit this *filesystem* argument, the system shows a list of the files on the file system specified by the **cd** command.

Examples

The following example shows that the present working file system specified by the **cd** command is slot 0:

```
Router> pwd
slot0:/
```

The following example uses the **cd** command to change the present file system to slot 1 and then uses the **pwd** command to display that present working file system:

```
Router> cd slot1:
Router> pwd
slot1:/
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.

rename

To rename a file in a Class C Flash file system, use the **rename** EXEC command.

rename *url1 url2*

Syntax Description

url1	The original path and filename.
url2	The new path and filename.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is valid only on Class C Flash file systems.

Examples

In the following example, the file named Karen.1 is renamed test:

```
Router# dir

Directory of disk0:/Karen.dir/

  0  -rw-          0   Jan 21 1998 09:51:29  Karen.1
  0  -rw-          0   Jan 21 1998 09:51:29  Karen.2
  0  -rw-          0   Jan 21 1998 09:51:29  Karen.3
  0  -rw-          0   Jan 21 1998 09:51:31  Karen.4
243  -rw-        165   Jan 21 1998 09:53:17  Karen.cur

340492288 bytes total (328400896 bytes free)

Router# rename disk0:Karen.dir/Karen.1 disk0:Karen.dir/test
Router# dir

Directory of disk0:/Karen.dir/

  0  -rw-          0   Jan 21 1998 09:51:29  Karen.2
  0  -rw-          0   Jan 21 1998 09:51:29  Karen.3
  0  -rw-          0   Jan 21 1998 09:51:31  Karen.4
243  -rw-        165   Jan 21 1998 09:53:17  Karen.cur
  0  -rw-          0   Apr 24 1998 09:49:19  test

340492288 bytes total (328384512 bytes free)
```

rmdir

To remove an existing directory in a Class C Flash file system, use the **rmdir** EXEC command.

rmdir *directory*

Syntax Description

directory	Directory to delete.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

This command is valid only on Class C Flash file systems.

Examples

The following example deletes the directory named newdir:

```
Router# dir

Directory of flash:

  2  drwx           0   Mar 13 1993 13:16:21  newdir

8128000 bytes total (8126976 bytes free)
Router# rmdir newdir
Rmdir file name [newdir]?
Delete flash:newdir? [confirm]
Removed dir flash:newdir
Router# dir
Directory of flash:

No files in directory

8128000 bytes total (8126976 bytes free)
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
mkdir	Creates a new directory in a Class C Flash file system.

show configuration

The **show configuration** command is replaced by the **show startup-config** and **more nvram:startup-config** commands. See the description of the **show startup-config** and **more** commands for more information.

show file descriptors

To display a list of open file descriptors, use the **show file descriptors** EXEC command.

show file descriptors

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

File descriptors are the internal representations of open files. You can use this command to learn if another user has a file open.

Examples

The following is sample output from the **show file descriptors** command:

```
Router# show file descriptors

File Descriptors:

   FD  Position  Open   PID  Path
    0    187392  0001     2  tftp://dirt/hampton/c4000-i-m.a
    1    184320  030A     2  flash:c4000-i-m.a
```

Table 27 describes the significant fields shown in the display.

Table 27 show file descriptors Field Descriptions

Field	Description
FD	File descriptor. The file descriptor is a small integer used to specify the file once it has been opened.
Position	Byte offset from the start of the file.
Open	Flags supplied when opening the file.
PID	Process ID of the process that opened the file.
Path	Location of the file.

45233

show file information

To display information about a file, use the **show file information** EXEC command.

show file information *file-url*

Syntax Description

file-url	The URL of the file to display.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Examples

The following is sample output from the **show file information** command:

```
Router# show file information tftp://dirt/hampton/c2500-j-l.a

tftp://dirt/hampton/c2500-j-l.a:
  type is image (a.out) [relocatable, run from flash]
  file size is 8624596 bytes, run size is 9044940 bytes [8512316+112248+420344]
  Foreign image

Router# show file information slot0:c7200-js-mz

slot0:c7200-js-mz:
  type is image (elf) []
  file size is 4770316 bytes, run size is 4935324 bytes
  Runnable image, entry point 0x80008000, run from ram

Router1# show file information nvram:startup-config

nvram:startup-config:
  type is ascii text
```

Table 28 describes the possible file types.

Table 28 Possible File Types

Types	Description
image (a.out)	Runnable image in a.out format.
image (elf)	Runnable image in elf format.
ascii text	Configuration file or other text file.
coff	Runnable image in coff format.
ebcdic	Text generated on an IBM mainframe.
lzw compression	Lzw compressed file.
tar	Text archive file used by the Channel Interface Processor (CIP).

show file systems

To list available file systems, use the **show file systems** command in EXEC mode.

show file systems

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 AA	This command was introduced.

Usage Guidelines

Use this command to learn the alias names (Prefixes) of the file systems your router supports.

Examples

The following is sample output from the **show file systems** command:

```
Router# show file systems

File Systems:

     Size(b)       Free(b)     Type     Flags   Prefixes
           -             -   opaque     rw      null:
           -             -   opaque     rw      system:
           -             -   opaque     ro      xmodem:
           -             -   opaque     ro      ymodem:
           -             -  network     rw      tftp:
           -             -  network     rw      rcp:
           -             -  network     rw      ftp:
*    4194304       4190616    flash     rw      flash:
      131066        129185    nvram     rw      nvram:
           -             -   opaque     wo      lex:
```

Table 29 describes the significant fields shown in the display.

Table 29 show file systems Field Descriptions

Type	Description
Size(b)	Amount of memory in the file system (in bytes).
Free(b)	Amount of free memory in the file system (in bytes).
Type	Type of file system.
Flags	Permissions for file system.
Prefixes	Alias for file system.
disk	The file system is for a rotating medium.
flash	The file system is for a Flash memory device.

7521 3

Table 29 show file systems Field Descriptions (continued)

Type	Description
network	The file system is a network file system (TFTP, rcp, FTP, and so on).
nvram	The file system is for an NVRAM device.
opaque	The file system is a locally generated "pseudo" file system (for example, the "system") or a download interface, such as brimux.
rom	The file system is for a ROM or EPROM device.
tty	The file system is for a collection of terminal devices.
unknown	The file system is of unknown type.

Table 30 describes file system flags.

Table 30 Possible File System Flags

Flag	Description
ro	The file system is Read Only.
rw	The file system is Write Only.
wo	The file system is Read/Write.

squeeze

To permanently erase files tagged as "deleted" or "error" on Class A Flash file systems, use the **squeeze** command in EXEC mode.

squeeze [**/nolog**] [**/quiet**] *filesystem*:

Syntax Description

/nolog	(Optional) Disables the squeeze log (recovery data) and accelerates the squeeze process.
/quiet	(Optional) Disables status messages during the squeeze process.
filesystem:	The Flash file system, followed by a colon. Typically **flash:** or **slot0:**.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(1)	This command was implemented in images for the Cisco 2600 and Cisco 3600 series.
12.2(4)XL	This command was implemented in images for the Cisco 1700 series.
12.1(9), 12.0(17)S 12.0(17)ST, 12.2(2), 12.2(2)T, 12.2(2)B, 12.1(9)E	The **/nolog** and **/quiet** keywords were added.

Usage Guidelines

When Flash memory is full, you might need to rearrange the files so that the space used by the files marked "deleted" can be reclaimed. (This "squeeze" process is required for linear Flash memory cards to make sectors contiguous; the free memory must be in a "block" to be usable.)

When you enter the **squeeze** command, the router copies all valid files to the beginning of Flash memory and erases all files marked "deleted." After the squeeze process is completed, you can write to the reclaimed Flash memory space.

Caution After performing the squeeze process you cannot recover deleted files using the **undelete** EXEC mode command.

In addition to removing deleted files, the **squeeze** command removes any files that the system has marked as "error". An error file is created when a file write fails (for example, the device is full). To remove error files, you must use the **squeeze** command.

Rewriting Flash memory space during the squeeze operation may take several minutes.

Using the **/nolog** keyword disables the log for the squeeze process. In most cases this will speed up the squeeze process. However, if power is lost or the Flash card is removed during the squeeze process, all the data on the Flash card will be lost, and the device will have to be reformatted.

Note Using the **/nolog** keyword makes the squeeze process uninterruptible.

Using the **/quiet** keyword disables the output of status messages to the console during the squeeze process.

If the optional keywords are not used, the progress of squeeze process will be displayed to the console, a log for the process will be maintained, and the squeeze process is interruptible.

On Cisco 2600 or Cisco 3600 series routers, the entire file system needs to be erased once before the **squeeze** command can be used. After being erased once, the **squeeze** command should operate properly on the Flash file system for the rest of the Flash file system's history.

To erase an entire flash file system on a Cisco 2600 or 3600 series router, perform the following steps:

Step 1 If the Flash file system has multiple partitions, enter the **no partition** command to remove the partitions. The reason for removing partitions is to ensure that the entire Flash file system is erased. The **squeeze** command can be used in a Flash file system with partitions after the Flash file system is erased once.

Step 2 Enter the **erase** command to erase the Flash file system.

Examples

In the following example, the file named "config1" is deleted, and then the **squeeze** command is used to reclaim the space used by that file. The **/nolog** option is used to speed up the squeeze process.

```
Router# delete config1
Delete filename [config1]?
Delete slot0:conf? [confirm]
Router# dir slot0:
! Note that the deleted file name appears in square brackets
Directory of slot0:/

    1  -rw-     4300244   Apr 02 2001 03:18:07  c7200-boot-mz.122-0.14
    2  -rw-        2199   Apr 02 2001 04:45:15  [config1]
    3  -rw-     4300244   Apr 02 2001 04:45:23  image
20578304 bytes total (11975232 bytes free)
!20,578,304 - 4,300,244 - 4,300,244 - 2,199 - 385 = 11975232


Router# squeeze /nolog slot0:
%Warning: Using /nolog option would render squeeze operation uninterruptible.
All deleted files will be removed. Continue? [confirm]
Squeeze operation may take a while. Continue? [confirm]

Squeeze of slot0 completed in 291.832 secs .
Router# dir slot0:
Directory of slot0:/

    1  -rw-     4300244   Apr 02 2001 03:18:07  c7200-boot-mz.122-0.14
    2  -rw-     4300244   Apr 02 2001 04:45:23  image

20578304 bytes total (11977560 bytes free)
!20,578,304 - 4,300,244 - 4,300,244 - 256 = 11977560
```

Related Commands

Command	Description
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
undelete	Recovers a file marked "deleted" on a Class A or Class B Flash file system.

undelete

To recover a file marked "deleted" on a Class A or Class B Flash file system, use the **undelete** EXEC command.

undelete *index* [*filesystem*:]

Syntax Description

index	A number that indexes the file in the **dir** command output.
filesystem:	(Optional) A file system containing the file to undelete, followed by a colon.

Defaults

The default file system is the one specified by the **cd** command.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

For Class A and B Flash file systems, when you delete a file, the Cisco IOS software simply marks the file as deleted, but it does not erase the file. This command allows you to recover a "deleted" file on a specified Flash memory device. You must undelete a file by its index because you could have multiple deleted files with the same name. For example, the "deleted" list could contain multiple configuration files with the name router-config. You undelete by index to indicate which of the many router-config files from the list to undelete. Use the **dir** command to learn the index number of the file you want to undelete.

You cannot undelete a file if a valid (undeleted) file with the same name exists. Instead, you first delete the existing file and then undelete the file you want. For example, if you had an undeleted version of the router-config file and you wanted to use a previous, deleted version instead, you could not simply undelete the previous version by index. You would first delete the existing router-config file and then undelete the previous router-config file by index. You can delete and undelete a file up to 15 times.

On Class A Flash file systems, if you try to recover the configuration file pointed to by the CONFIG_FILE environment variable, the system prompts you to confirm recovery of the file. This prompt reminds you that the CONFIG_FILE environment variable points to an undeleted file. To permanently delete all files marked "deleted" on a Flash memory device, use the **squeeze** EXEC command.

On Class B Flash file systems, you must use the **erase** EXEC command to recover any space taken up by deleted files.

Examples

The following example recovers the deleted file whose index number is 1 to the Flash memory card inserted in slot 0:

```
undelete 1 slot0:
```

Related Commands

Command	Description
delete	Deletes a file on a Flash memory device.
dir	Displays a list of files on a file system.
squeeze	Permanently deletes Flash files by squeezing a Class A Flash file system.

4515
3

verify

To verify the checksum of a file on a Flash memory file system, use the **verify** EXEC command.

verify *filesystem*:[*file-url*]

Syntax Description

filesystem:	Flash memory file system containing the files to list, followed by a colon. Standard file system keywords for this command include **flash:**, **bootflash:**, and **slot0:**.
file-url	(Optional) URL of the file to verify. Generally this consists only of the filename(s), but you may also specify directories (file paths), separated by forward-slashes (/). The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Defaults

The current working device is the default device.

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command replaces the **copy verify** and **copy verify flash** commands.

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into Flash memory; it is not displayed when the image file is copied from one disk to another.

To display the contents of Flash memory, use the **show flash** command. The Flash contents listing dc not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into Flash memory, use the **verify** command.

Note The verify command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the router and saved in the file system without detection.
To verify that a Cisco IOS software image was not corrupted while it was transfered to the router, copy the image from where it is stored on your router to a Unix server. Also copy the same image from CCO (Cisco.com) to the same Unix server. (The name may need to be modified if you try to save the image in the same directory as the image that you copied from the router.) Then run a Unix **diff** command on the two Cisco IOS software images. If there is no difference then the image stored on the router has not been corrupted.

Examples

The following example verifies that the file named c7200-js-mz is on the Flash memory card inserted in slot 0:

```
Router# dir slot0:
Directory of slot0:/

  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  5  -rw-         639   Oct 02 1997 12:09:32  rally
  7  -rw-         639   Oct 02 1997 12:37:13  the_time

20578304 bytes total (3104544 bytes free)
tw3-7200-1# verify slot0:
Verify filename []? c7200-js-mz
Verified slot0:
```

The following example also verifies that the file named c7200-js-mz is on the Flash memory card inserted in slot 0:

```
Router# verify slot0:?
slot0:c7200-js-mz  slot0:rally slot0:hampton/nitro/c7200-j-mz  slot0:the_time

Router# verify slot0:c7200-js-mz
Verified slot0:c7200-js-mz
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination, use the copy EXEC command.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the **cd** command.
show file systems	Lists available file systems.

7513 E

write erase

The **write erase** command is replaced by the **erase nvram:** command. See the description of the **erase** command in this chapter for more information.

write terminal

The **more system:running-config** command replaces the **write terminal** command. See the description of the **more** command in this chapter for more information.

AP. GJ

Configuring BGP

This chapter describes how to configure Border Gateway Protocol (BGP). For a complete description of the BGP commands in this chapter, refer to the "BGP Commands" chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online. For multiprotocol BGP configuration information and examples, refer to the "Configuring Multiprotocol BGP Extensions for IP Multicast" chapter of the *Cisco IOS IP Configuration Guide*. For multiprotocol BGP command descriptions, refer to the "Multiprotocol BGP Extensions for IP Multicast Commands" chapter of the *Cisco IOS IP Command Reference*.

BGP, as defined in RFCs 1163 and 1267, is an Exterior Gateway Protocol (EGP). It allows you to set up an interdomain routing system that automatically guarantees the loop-free exchange of routing information between autonomous systems.

For protocol-independent features, see the chapter "Configuring IP Routing Protocol-Independent Features" in this book.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter in this book.

The Cisco BGP Implementation

In BGP, each route consists of a network number, a list of autonomous systems that information has passed through (called the *autonomous system path*), and a list of other *path attributes*. We support BGP Versions 2, 3, and 4, as defined in RFCs 1163, 1267, and 1771, respectively.

The primary function of a BGP system is to exchange network reachability information with other BGP systems, including information about the list of autonomous system paths. This information can be used to construct a graph of autonomous system connectivity from which routing loops can be pruned and with which autonomous system-level policy decisions can be enforced.

You can configure the value for the Multi Exit Discriminator (MED) metric attribute using route maps. (The name of this metric for BGP Versions 2 and 3 is INTER_AS_METRIC.) When an update is sent to an internal BGP (iBGP) peer, the MED is passed along without any change. This action enables all the peers in the same autonomous system to make a consistent path selection.

A next hop router address is used in the NEXT_HOP attribute, regardless of the autonomous system of that router. The Cisco IOS software automatically calculates the value for this attribute.

Transitive, optional path attributes are passed along to other BGP-speaking routers.

BGP Version 4 supports classless interdomain routing (CIDR), which lets you reduce the size of your routing tables by creating aggregate routes, resulting in *supernets*. CIDR eliminates the concept of network classes within BGP and supports the advertising of IP prefixes. CIDR routes can be carried by Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), and Intermediate System-to-Intermediate System (ISIS)-IP, and Routing Information Protocol (RIP).

See the "BGP Route Map Examples" section at the end of this chapter for examples of how to use route maps to redistribute BGP Version 4 routes.

How BGP Selects Paths

A router running Cisco IOS Release 12.0 or later does not select or use an iBGP route unless both of the following conditions are true:

- The router has a route available to the next hop router:
- The router has received synchronization via an IGP (unless IGP synchronization has been disabled).

BGP bases its decision process on the attribute values. When faced with multiple routes to the same destination, BGP chooses the best route for routing traffic toward the destination. The following process summarizes how BGP chooses the best route.

1. If the next hop is inaccessible, do not consider it.

   This decision is why it is important to have an IGP route to the next hop.

2. If the path is internal, synchronization is enabled, and the route is not in the IGP, do not consider the route.
3. Prefer the path with the largest weight (weight is a Cisco proprietary parameter).
4. If the routes have the same weight, prefer the route with the largest local preference.
5. If the routes have the same local preference, prefer the route that was originated by the local router.

   For example, a route might be originated by the local router using the **network bgp** router configuration command, or through redistribution from an IGP.

6. If the local preference is the same, or if no route was originated by the local router, prefer the route with the shortest autonomous system path.
7. If the autonomous system path length is the same, prefer the route with the lowest origin code (IGP < EGP < INCOMPLETE).
8. If the origin codes are the same, prefer the route with the lowest MED metric attribute.

   This comparison is only made if the neighboring autonomous system is the same for all routes considered, unless the **bgp always-compare-med** router configuration command is enabled.

   Note The most recent Internet Engineering Task Force (IETF) decision regarding BGP MED assigns a value of infinity to the missing MED, making the route lacking the MED variable the least preferred. The default behavior of BGP routers running Cisco IOS software is to treat routes without the MED attribute as having a MED of 0, making the route lacking the MED variable the most preferred. To configure the router to conform to the IETF standard, use the **bgp bestpath med missing-as-worst** router configuration command.

9. Prefer the external BGP (eBGP) path over the iBGP path.

   All confederation paths are considered internal paths.

10. Prefer the route that can be reached through the closest IGP neighbor (the lowest IGP metric).

    The router will prefer the shortest internal path within the autonomous system to reach the destination (the shortest path to the BGP next hop).

11. If the following conditions are all true, insert the route for this path into the IP routing table:
    - Both the best route and this route are external.
    - Both the best route and this route are from the same neighboring autonomous system.
    - The **maximum-paths** router configuration command is enabled.

    Note eBGP load sharing can occur at this point, which means that multiple paths can be installed in the forwarding table.

12. If multipath is not enabled, prefer the route with the lowest IP address value for the BGP router ID.

    The router ID is usually the highest IP address on the router or the loopback (virtual) address, but might be implementation-specific.

BGP Multipath Support

When a BGP speaker learns two identical eBGP paths for a prefix from a neighboring autonomous system, it will choose the path with the lowest route ID as the best path. This best path is installed in the IP routing table. If BGP multipath support is enabled and the eBGP paths are learned from the same neighboring autonomous system, instead of one best path being picked, multiple paths are installed in the IP routing table.

During packet switching, depending on the switching mode, either per-packet or per-destination load balancing is performed among the multiple paths. A maximum of six paths is supported. The **maximum-paths** router configuration command controls the number of paths allowed. By default, BGP will install only one path to the IP routing table.

Basic BGP Configuration Task List

The BGP configuration tasks are divided into basic and advanced tasks, which are described in the following sections. The basic tasks described in the first two sections are required to configure BGP; the basic and advanced tasks in the remaining sections are optional:

- Enabling BGP Routing (Required)
- Configuring BGP Neighbors (Required)
- Managing Routing Policy Changes (Optional)
- Verifying BGP Soft Reset (Optional)
- Configuring BGP Interactions with IGPs (Optional)
- Configuring BGP Weights (Optional)
- Disabling Autonomous System Path Comparison (Optional)
- Configuring BGP Route Filtering by Neighbor (Optional)
- Configuring BGP Filtering Using Prefix Lists (Optional)
- Configuring BGP Path Filtering by Neighbor (Optional)

- Disabling Next Hop Processing on BGP Updates (Optional)
- Configuring the BGP Version (Optional)
- Configuring the MED Metric (Optional)

Advanced BGP Configuration Task List

Advanced, optional BGP configuration tasks are described in the following sections:

- Using Route Maps to Modify Updates (Optional)
- Resetting eBGP Connections Immediately upon Link Failure (Optional)
- Configuring Aggregate Addresses (Optional)
- Disabling Automatic Summarization of Network Numbers (Optional)
- Configuring BGP Community Filtering (Optional)
- Configuring BGP Conditional Advertisement (Optional)
- Configuring a Routing Domain Confederation (Optional)
- Configuring a Route Reflector (Optional)
- Configuring BGP Peer Groups (Optional)
- Disabling a Peer or Peer Group (Optional)
- Indicating Backdoor Routes (Optional)
- Modifying Parameters While Updating the IP Routing Table (Optional)
- Setting Administrative Distance (Optional)
- Adjusting BGP Timers (Optional)
- Changing the Default Local Preference Value (Optional)
- Redistributing Network 0.0.0.0 (Optional)
- Configuring the Router to Consider a Missing MED as Worst Path (Optional)
- Selecting Path Based on MEDs from Other Autonomous Systems (Optional)
- Configuring the Router to Use the MED to Choose a Path from Subautonomous System Paths (Optional)
- Configuring the Router to Use the MED to Choose a Path in a Confederation (Optional)
- Configuring Route Dampening (Optional)

For information on configuring features that apply to multiple IP routing protocols (such as redistributing routing information), see the chapter "Configuring IP Routing Protocol-Independent Features."

Configuring Basic BGP Features

The tasks described in this section are for configuring basic BGP features.

Enabling BGP Routing

To enable BGP routing and establish a BGP routing process, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **router bgp** *as-number*	Enables a BGP routing process, which places the router in router configuration mode.
Step 2	Router(config-router)# **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]	Flags a network as local to this autonomous system and enters it to the BGP table.

Note For exterior protocols, a reference to an IP network from the **network** router configuration command controls only which networks are advertised. This behavior is in contrast to IGP, such as IGRP, which also use the **network** command to determine where to send updates.

Note The **network** command is used to inject IGP routes into the BGP table. The *network-mask* portion of the command allows supernetting and subnetting. The resources of the router, such as configured NVRAM or RAM, determine the upper limit of the number of **network** commands you can use. Alternatively, you could use the **redistribute** router configuration command to achieve the same result.

Configuring BGP Neighbors

Like other EGPs, BGP must completely understand the relationships it has with its neighbors. Therefore, this task is required.

BGP supports two kinds of neighbors: internal and external. *Internal neighbors* are in the same autonomous system; *external neighbors* are in different autonomous systems. Normally, external neighbors are adjacent to each other and share a subnet, while internal neighbors may be anywhere in the same autonomous system.

To configure BGP neighbors, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*	Specifies a BGP neighbor.

See the "BGP Neighbor Configuration Examples" section at the end of this chapter for an example of configuring BGP neighbors.

Managing Routing Policy Changes

Routing policies for a peer include all the configurations such as route-map, distribute-list, prefix-list, and filter-list that may impact inbound or outbound routing table updates. Whenever there is a change in the routing policy, the BGP session must be soft cleared, or soft reset, for the new policy to take effect. Performing inbound reset enables the new inbound policy to take effect. Performing outbound reset causes the new local outbound policy take effect without resetting the BGP session. As a new set of updates is sent during outbound policy reset, a new inbound policy of the neighbor can also take effect.

There are two types of reset, hard reset and soft reset. Table 8 lists their advantages and disadvantages.

Table 8 Advantages and Disadvantages of Hard and Soft Resets

Type of Reset	Advantages	Disadvantages
Hard reset	No memory overhead.	The prefixes in the BGP, IP, and Forwarding Information Base (FIB) tables provided by the neighbor are lost. Not recommended.
Outbound soft reset	No configuration, no storing of routing table updates. The procedure for an outbound reset is described in the section "Configuring BGP Soft Reset Using Stored Routing Policy Information."	Does not reset inbound routing table updates.
Dynamic inbound soft reset	Does not clear the BGP session and cache. Does not require storing of routing table updates, and has no memory overhead.	Both BGP routers must support the route refresh capability (in Cisco IOS Release 12.1 and later releases).
Configured inbound soft reset (uses the **neighbor soft-reconfiguration** router configuration command)	Can be used when both BGP routers do not support the automatic route refresh capability.	Requires preconfiguration. Stores all received (inbound) routing policy updates without modification; is memory-intensive. Recommended only when absolutely necessary, such as when both BGP routers do not support the automatic route refresh capability.

Once you have defined two routers to be BGP neighbors, they will form a BGP connection and exchange routing information. If you subsequently change a BGP filter, weight, distance, version, or timer, or make a similar configuration change, you must reset BGP connections for the configuration change to take effect.

A soft reset updates the routing table for inbound and outbound routing updates. Cisco IOS software Release 12.1 and later releases support soft reset without any prior configuration. This soft reset allows the dynamic exchange of route refresh requests and routing information between BGP routers, and the subsequent re-advertisement of the respective outbound routing table. There are two types of soft reset:

- When soft reset is used to generate inbound updates from a neighbor, it is called dynamic inbound soft reset.
- When soft reset is used to send a new set of updates to a neighbor, it is called outbound soft reset.

To use soft reset without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the OPEN message sent when the peers establish a TCP session. Routers running Cisco IOS software releases prior to Release 12.1 do not support the route refresh capability and must clear the BGP session using the **neighbor soft-reconfiguration** router configuration command, described in "Configuring BGP Soft Reset Using Stored Routing Policy Information." Clearing the BGP session in this way will have a negative impact upon network operations and should only be used as a last resort.

Resetting a Router Using BGP Dynamic Inbound Soft Reset

If both the local BGP router and the neighbor router support the route refresh capability, you can perform a dynamic soft inbound reset. This type of reset has the following advantages over a soft inbound reset using stored routing update information:

- Does not require preconfiguration
- Does not require additional memory for storing routing update information

To determine whether a router supports the route refresh capability, use the **show ip bgp neighbors** command in EXEC mode:

Command	Purpose
Router# **show ip bgp neighbors** *ip-address*	Displays whether a neighbor supports the route refresh capability. If the specified router supports the route refresh capability, the following message is displayed: Received route refresh capability from peer.

If all the BGP routers support the route refresh capability, you can use the dynamic soft reset method for resetting the inbound routing table. To perform a dynamic soft reset of the inbound routing table, use the following command in EXEC mode:

Command	Purpose
Router# **clear ip bgp** {***** | *neighbor-address* | *peer-group-name*} **soft in**	Performs a dynamic soft reset on the connection specified in the command. The *neighbor-address* argument specifies the connection to be reset. Use the ***** keyword to specify that all connections be reset.

See the "BGP Soft Reset Examples" section at the end of this chapter for examples of both types of BGP soft resets.

Resetting a Router Using BGP Outbound Soft Reset

Outbound soft resets do not require any preconfiguration. Using the **soft** keyword specifies that a soft reset be performed. To perform an outbound soft reset, use the following command in EXEC mode:

Command	Purpose
`Router# clear ip bgp {*	neighbor-address	peer-group-name} soft out`	Performs a soft reset on the connection specified in the command. The *neighbor-address* argument specifies the connection to be reset. Use the * keyword to specify that all connections be reset.

Configuring BGP Soft Reset Using Stored Routing Policy Information

If all of the BGP routers in the connection do not support the route refresh capability, use the soft reset method that generates a new set of inbound routing table updates from information previously stored. To initiate storage of inbound routing table updates, you must first preconfigure the router using the **neighbor soft-reconfiguration** router configuration command. The **clear ip bgp EXEC** command initiates the soft reset, which generates a new set of inbound routing table updates using the stored information.

Remember that the memory requirements for storing the inbound update information can become quite large.To configure BGP soft reset using stored routing policy information, use the following commands beginning in router configuration mode:

	Command	Purpose
Step 1	`Router(config-router)# neighbor {ip-address	peer-group-name} soft-reconfiguration inbound`	Resets the BGP session and initiates storage of inbound routing table updates from the specified neighbor or peer group. From that point forward, a copy of the BGP routing table for the specified neighbor or peer group is maintained on the router. The Cisco implementation of BGP supports BGP Versions 2, 3, and 4. If the neighbor does not accept default Version 4, dynamic version negotiation is implemented to negotiate down to Version 2. If you specify a BGP peer group by using the *peer-group-name* argument, all members of the peer group will inherit the characteristic configured with this command.
Step 2	`Router# clear ip bgp {*	neighbor-address	peer-group-name} soft in`	Performs a soft reset on the connection specified in the command, using the stored routing table information for that connection.

See the "BGP Path Filtering by Neighbor Examples" section at the end of this chapter for an example of BGP path filtering by neighbor.

Verifying BGP Soft Reset

To verify whether a soft reset is successful and check information about the routing table and about BGP neighbors, perform the following steps:

Step 1 Enter the **show ip bgp** EXEC command to display entries in the BGP routing table. The following output shows that the peer supports the route refresh capability:

```
Router# show ip bgp

BGP table version is 5, local router ID is 10.0.33.34
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0          0.0.0.0                  0         32768 ?
*  2.0.0.0          10.0.33.35              10             0 35 ?
*>                  0.0.0.0                  0         32768 ?
*  10.0.0.0         10.0.33.35              10             0 35 ?
*>                  0.0.0.0                  0         32768 ?
*> 192.168.0.0/16   10.0.33.35              10             0 35 ?
```

Step 2 Enter the **show ip bgp neighbors** EXEC command to display information about the BGP and TCP connections to neighbors:

```
Router# show ip bgp neighbors 171.69.232.178

BGP neighbor is 172.16.232.178,  remote AS 35, external link
  BGP version 4, remote router ID 192.168.3.3
  BGP state = Established, up for 1w1d
  Last read 00:00:53, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Multicast: advertised and received
  Received 12519 messages, 0 notifications, 0 in queue
  Sent 12523 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is uni-in
  Route map for outgoing advertisements is uni-out
  3 accepted prefixes consume 108 bytes
  Prefix advertised 6, suppressed 0, withdrawn 0

 For address family: IPv4 Multicast
  BGP table version 5, neighbor version 5
  Index 1, Offset 0, Mask 0x2
  Inbound path policy configured
  Outbound path policy configured
  Route map for incoming advertisements is mul-in
  Route map for outgoing advertisements is mul-out
  3 accepted prefixes consume 108 bytes
  Prefix advertised 6, suppressed 0, withdrawn 0

  Connections established 2; dropped 1
  Last reset 1w1d, due to Peer closed the session
```

```
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 172.16.232.178, Local port: 179
Foreign host: 172.16.232.179, Foreign port: 11002

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x2CF49CF8):
Timer          Starts    Wakeups            Next
Retrans         12518          0             0x0
TimeWait            0          0             0x0
AckHold         12514      12281             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss:  273358651  snduna:  273596614  sndnxt:  273596614     sndwnd:  15434
irs:  190480283  rcvnxt:  190718186  rcvwnd:      15491  delrcvwnd:    893

SRTT: 300 ms, RTTO: 607 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 1460 bytes):
Rcvd: 24889 (out of order: 0), with data: 12515, total data bytes: 237921
Sent: 24963 (retransmit: 0), with data: 12518, total data bytes: 237981
```

Configuring BGP Interactions with IGPs

If your autonomous system will be passing traffic through it from another autonomous system to a third autonomous system, make sure that your autonomous system is consistent about the routes that it advertises. For example, if your BGP were to advertise a route before all routers in your network had learned about the route through your IGP, your autonomous system could receive traffic that some routers cannot yet route. To prevent this condition from occurring, BGP must wait until the IGP has propagated routing information across your autonomous system, thus causing BGP to be synchronized with the IGP. Synchronization is enabled by default.

In some cases, you need not synchronize. If you will not be passing traffic from a different autonomous system through your autonomous system, or if all routers in your autonomous system will be running BGP, you can disable synchronization. Disabling this feature can allow you to carry fewer routes in your IGP and allow BGP to converge more quickly. To disable synchronization, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no synchronization`	Disables synchronization between BGP and an IGP.

See the "BGP Path Filtering by Neighbor Examples" section at the end of this chapter for an example of BGP synchronization.

In general, you will not want to redistribute most BGP routes into your IGP. A common design is to redistribute one or two routes and to make them exterior routes in IGRP, or have your BGP speaker generate a default route for your autonomous system. When redistributing from BGP into IGP, only the routes learned using eBGP get redistributed.

In most circumstances, you also will not want to redistribute your IGP into BGP. List the networks in your autonomous system with **network** router configuration commands and your networks will be advertised. Networks that are listed this way are referred to as *local networks* and have a BGP origin attribute of "IGP." They must appear in the main IP routing table and can have any source; for example, they can be directly connected or learned via an IGP. The BGP routing process periodically scans the main IP routing table to detect the presence or absence of local networks, updating the BGP routing table as appropriate.

If you do perform redistribution into BGP, you must be very careful about the routes that can be in your IGP, especially if the routes were redistributed from BGP into the IGP elsewhere. Redistributing routes from BGP into the IGP elsewhere creates a situation where BGP is potentially injecting information into the IGP and then sending such information back into BGP, and vice versa. Incorrectly redistributing routes into BGP can result in the loss of critical information, such as the autonomous system path, that is required for BGP to function properly.

Networks that are redistributed into BGP from the EGP protocol will be given the BGP origin attribute "EGP." Other networks that are redistributed into BGP will have the BGP origin attribute of "incomplete." The origin attribute in the Cisco implementation is only used in the path selection process.

Configuring BGP Weights

A weight is a number that you can assign to a path so that you can control the path selection process. The administrative weight is local to the router. A weight can be a number from 0 to 65535. Any path that a Cisco router originates will have a default weight of 32768; other paths have weight 0. If you have particular neighbors that you want to prefer for most of your traffic, you can assign a higher weight to all routes learned from that neighbor.

Weights can be assigned based on autonomous system path access lists. A given weight becomes the weight of the route if the autonomous system path is accepted by the access list. Any number of weight filters are allowed. Weights can only be assigned via route maps.

Disabling Autonomous System Path Comparison

RFC 1771, the IETF document defining BGP, does not include autonomous system path as part of the "tie-breaker" decision algorithm. By default, Cisco IOS software considers the autonomous system path as a part of the decision algorithm. This enhancement makes it possible to modify the decision algorithm, bringing the behavior of the router in selecting a path more in line with the IETF specification.

To prevent the router from considering the autonomous system path length when selecting a route, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp bestpath as-path ignore`	Configures the router to ignore autonomous system path length in selecting a route.

Configuring BGP Route Filtering by Neighbor

You can filter BGP advertisements in two ways:

- Use autonomous system path filters, as with the **ip as-path access-list** global configuration command and the **neighbor filter-list** router configuration command
- Use access or prefix lists, as with the **neighbor distribute-list** router configuration command.

Filtering using prefix lists is described in the "Configuring BGP Filtering Using Prefix Lists" section.

If you want to restrict the routing information that the Cisco IOS software learns or advertises, you can filter BGP routing updates to and from particular neighbors. You can either define an access list or a prefix list and apply it to the updates.

Note Distribute-list filters are applied to network numbers and not autonomous system paths.

To filter BGP routing updates, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *access-list-name*} {**in** | **out**}	Filters BGP routing updates to and from neighbors as specified in an access list. **Note** The **neighbor prefix-list** router configuration command can be used as an alternative to the **neighbor distribute-list** router configuration command, but you cannot use both commands to configure the same BGP peer in any specific direction. These two commands are mutually exclusive, and only one command (**neighbor prefix-list** or **neighbor distribute-list**) an be applied for each inbound or outbound direction.

Note Although the **neighbor prefix-list** router configuration command can be used as an alternative to the **neighbor distribute-list** command, do not use attempt to apply both the **neighbor prefix-list** and **neighbor distribute-list** command filtering to the same neighbor in any given direction. These two commands are mutually exclusive, and only one command (**neighbor prefix-list** or **neighbor distribute-list**) can be applied for each inbound or outbound direction.

Configuring BGP Filtering Using Prefix Lists

Prefix lists can be used as an alternative to access lists in many BGP route filtering commands. The section "How the System Filters Traffic by Prefix List" describes the way prefix list filtering works. The advantages of using prefix lists are as follows:

- Significant performance improvement in loading and route lookup of large lists.
- Support for incremental updates. Filtering using extended access lists does not support incremental updates.

- More user-friendly command-line interface (CLI). The command-line interface for using access lists to filter BGP updates is difficult to understand and use because it uses the packet filtering format.
- Greater flexibility

Before using a prefix list in a command, you must set up a prefix list, and you may want to assign sequence numbers to the entries in the prefix list.

How the System Filters Traffic by Prefix List

Filtering by prefix list involves matching the prefixes of routes with those listed in the prefix list. When there is a match, the route is used. More specifically, whether a prefix is permitted or denied is based upon the following rules:

- An empty prefix list permits all prefixes.
- An implicit deny is assumed if a given prefix does not match any entries of a prefix list.
- When multiple entries of a prefix list match a given prefix, the longest, most specific match is chosen.

  The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router need not go through the rest of the prefix list. For efficiency, you may want to put the most common matches or denies near the top of the list, using the **seq** argument in the **ip prefix-list** global configuration command. The **show** commands always include the sequence numbers in their output.

Sequence numbers are generated automatically unless you disable this automatic generation. If you disable the automatic generation of sequence numbers, you must specify the sequence number for each entry using the *sequence-value* argument of the **ip prefix-list** global configuration command.

Regardless of whether the default sequence numbers are used in configuring a prefix list, a sequence number need not be specified when removing a configuration entry.

show commands include the sequence numbers in their output.

Creating a Prefix List

To create a prefix list, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# ip prefix-list list-name [seq sequence-value] {deny	permit network/length} [ge ge-value] [le le-value]`	Creates a prefix list with the name specified for the *list-name* argument.

Note To create a prefix list you must enter at least one **permit** or **deny** clause.

To remove a prefix list and all of its entries, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no ip prefix-list list-name [seq sequence-value] {deny	permit network/length} [ge ge-value] [le le-value]`	Removes a prefix list with the name specified for *list-name*.

7497
3

Configuring a Prefix List Entry

You can add entries to a prefix list individually. To configure an entry in a prefix list, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)#` **`ip prefix-list`** *`list-name`* `[`**`seq`** *`sequence-value`*`] {`**`deny`** `|` **`permit`** *`network/length`*`} [`**`ge`** *`ge-value`*`] [`**`le`** *`le-value`*`]`	Creates an entry in a prefix list and assigns a sequence number to the entry.

The optional **ge** and **le** keywords can be used to specify the range of the prefix length to be matched for prefixes that are more specific than the *network/length* argument. An exact match is assumed when neither **ge** nor **le** is specified. The range is assumed to be from *ge-value* to 32 if only the **ge** attribute is specified, and from **len** to *le-value* if only the **le** attribute is specified.

A specified *ge-value* or *le-value* must satisfy the following condition:

```
len < ge-value <= le-value <= 32
```

For example, to deny all prefixes matching /24 in 128.0.0.0/8, use the following command:

```
ip prefix-list abc deny  128.0.0.0/8 ge 24 le 24
```

Note You can specify sequence values for prefix list entries in any increments you want (the automatically generated numbers are incremented in units of 5). If you specify the sequence values in increments of 1, you cannot insert additional entries into the prefix list. If you choose very large increments, you could run out of sequence values.

Configuring How Sequence Numbers of Prefix List Entries Are Specified

By default, the sequence numbers are automatically generated when you create a prefix list entry. Sequence numbers can be suppressed with the **no ip prefix-list sequence-number** global configuration command. Sequence values are generated in increments of 5. The first sequence value generated in a prefix list would be 5, then 10, then 15, and so on. If you specify a value for an entry and then do not specify values for subsequent entries, the assigned (generated) sequence values are incremented in units of five. For example, if you specify that the first entry in the prefix list has a sequence value of 3, and then do not specify sequence values for the other entries, the automatically generated numbers will be 8, 13, 18, and so on.

To disable the automatic generation of sequence numbers, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)#` **`no ip prefix-list sequence-number`**	Disables the automatic generation of the sequence numbers for prefix list entries.

To re-enable automatic generation of the sequence numbers of prefix list entries, use the **ip prefix-list sequence number** command in router configuration mode:

Command	Purpose
Router(config-router)# **ip prefix-list sequence-number**	Enables the automatic generation of the sequence numbers of prefix list entries. The default is enable.

If you disable automatic generation of sequence numbers in a prefix list, you must specify the sequence number for each entry using the *sequence-value* argument of the **ip prefix-list** global configuration command.

Regardless of whether the default sequence numbers are used in configuring a prefix list, a sequence number need not be specified when deconfiguring an entry. **show** commands include the sequence numbers in their output.

Deleting a Prefix List or Prefix List Entries

To delete a prefix list, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **no ip prefix-list** *list-name*	Deletes a prefix list.

You can delete entries from a prefix list individually. To delete an entry in a prefix list, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **no ip prefix-list seq** *sequence-value*	Deletes an entry in a prefix list.

Note The sequence number of an entry need not be specified when you delete the entry.

Displaying Prefix Entries

To display information about prefix tables, prefix table entries, the policy associated with a node, or specific information about an entry, use the following commands in EXEC mode as needed:

Command	Purpose
Router# **show ip prefix-list** [**detail** | **summary**]	Displays information about all prefix lists.
Router# **show ip prefix-list** [**detail** | **summary**] *prefix-list-name*	Displays a table showing the entries in a prefix list.
Router# **show ip prefix-list** *prefix-list-name* [*network*/*length*]	Displays the policy associated with the node.
Router# **show ip prefix-list** *prefix-list-name* [**seq** *sequence-number*]	Displays the prefix list entry with a given sequence number.

7495.6

Router# **show ip prefix-list** *prefix-list-name* [*network/length*] **longer**	Displays all entries of a prefix list that are more specific than the given network and length.
Router# **show ip prefix-list** *prefix-list-name* [*network/length*] **first-match**	Displays the entry of a prefix list that matches the given prefix (network and length of prefix).

Clearing the Hit Count Table of Prefix List Entries

To clear the hit count table of prefix list entries, use the following command in EXEC mode:

Command	Purpose
Router# **clear ip prefix-list** *prefix-list-name* [*network/length*]	Clears the hit count table of the prefix list entries.

Configuring BGP Path Filtering by Neighbor

In addition to filtering routing updates based on network numbers, you can specify an access list filte: on both incoming and outbound updates based on the BGP autonomous system paths. Each filter is an access list based on regular expressions. To specify the access list filter, define an autonomous system path access list and apply it to updates to and from particular neighbors. See the "Regular Expressions" appendix in the *Cisco IOS Terminal Services Configuration Guide* for more information on forming regular expressions.

To configure BGP path filtering, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router# **ip as-path access-list** *access-list-number* {**permit** | **deny**} *as-regexp*	Defines a BGP-related access list.
Step 2	Router# **router bgp** *as-number*	Enters router configuration mode.
Step 3	Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}	Establishes a BGP filter.

See the "BGP Path Filtering by Neighbor Examples" section at the end of this chapter for an example of BGP path filtering by neighbor.

Disabling Next Hop Processing on BGP Updates

You can configure the Cisco IOS software to disable next hop processing for BGP updates to a neighbor. Disabling next hop processing might be useful in nonmeshed networks such as Frame Relay or X.25, where BGP neighbors might not have direct access to all other neighbors on the same IP subnet. There are two ways to disable next hop processing:

- Provide a specific address to be used instead of the next hop address (manually configuring each address).
- Use a route map to specify that the address of the remote peer for matching inbound routes, or the local router for matching outbound routes (automatic method).

Disabling Next Hop Processing Using a Specific Address

To disable next hop processing and provide a specific address to be used instead of the next hop address, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} next-hop-self`	Disables next hop processing on BGP updates to a neighbor.

Configuring this command causes the current router to advertise its peering address as the next hop for the specified neighbor. Therefore, other BGP neighbors will forward to it packets for that address. This configuration is useful in a nonmeshed environment because you know that a path exists from the present router to that address. In a fully meshed environment, this configuration is not useful because it will result in unnecessary extra hops and because there might be a direct access through the fully meshed cloud with fewer hops.

Disabling Next Hop Processing Using a Route Map

To override the inbound next hop setting for BGP routes and specify that the next hop of the matching routes is to be the IP address of the remote peer, or to set the peering address of the local router to be the next hop of the matching routes, use the **neighbor next-hop-self** router configuration command.

To configure the neighbor peering address to be used for the next hop address, use the following command in route map configuration mode:

Command	Purpose
`Router(config-route-map)# set ip next-hop ip-address [...ip-address] [peer-address]`	In an inbound route map of a BGP peer, sets the next hop of the matching routes to be the neighbor peering address, overriding any third-party next hops and allowing the same route map to be applied to multiple BGP peers to override third-party next hops. With an outbound route map of a BGP peer, sets the next hop of the received address to the peering address of the local router, disabling the next hop calculation. The next hop must be an adjacent router.

Configuring the BGP Version

By default, BGP sessions begin using BGP Version 4 and negotiating downward to earlier versions if necessary. To prevent negotiation and force the BGP version used to communicate with a neighbor, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address | peer-group-name} version number`	Specifies the BGP version to use when communicating with a neighbor.

Configuring the MED Metric

BGP uses the MED metric as a hint to external neighbors about preferred paths. (The name of this metric for BGP Versions 2 and 3 is INTER_AS_METRIC.) To set the MED of the redistributed routes, Use the following command in router configuration mode. All the routes without a MED will also be set to this value.

Command	Purpose
`Router(config-router)# default-metric number`	Sets an MED.

Alternatively, you can set the MED using the **route-map** router configuration command. See the "BGP Route Map Examples" section at the end of this chapter for examples of using BGP route maps.

Configuring Advanced BGP Features

The tasks in this section are for configuring advanced BGP features.

Using Route Maps to Modify Updates

You can use a route map on a per-neighbor basis to filter updates and modify various attributes. A route map can be applied to either inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates.

On both the inbound and the outbound updates, we support matching based on autonomous system path, community, and network numbers. Autonomous system path matching requires the **as-path access-list** global configuration command, community based matching requires the **ip community-list** global configuration command and network-based matching requires the **ip access-list** global configuration command. To apply a route map to incoming and outgoing routes, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor {ip-address	peer-group-name} route-map map-name {in	out}`	Applies a route map to incoming or outgoing routes.

See the "BGP Route Map Examples" section at the end of this chapter for BGP route map examples.

Resetting eBGP Connections Immediately upon Link Failure

Normally, when a link between external neighbors goes down, the BGP session will not be reset immediately.To reset the eBGP session as soon as an interface goes down, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp fast-external-fallover`	Resets eBGP sessions automatically.

Configuring Aggregate Addresses

CIDR enables you to create aggregate routes (or *supernets*) to minimize the size of routing tables. You can configure aggregate routes in BGP either by redistributing an aggregate route into BGP or by using the BGP Conditional Aggregation feature. An aggregate address will be added to the BGP table if at least one more specific entry is in the BGP table.

To create an aggregate address in the routing table, use the following commands in router configuration mode:

Command	Purpose
`Router(config-router)# aggregate-address address mask`	Creates an aggregate entry in the BGP routing table.
`Router(config-router)# aggregate-address address mask as-set`	Generates autonomous system set path information.
`Router(config-router)# aggregate-address address-mask summary-only`	Advertises summary addresses only.
`Router(config-router)# aggregate-address address mask suppress-map map-name`	Suppresses selected, more specific routes.
`Router(config-router)# aggregate-address address mask advertise-map map-name`	Generates an aggregate based on conditions specified by the route map.
`Router(config-router)# aggregate-address address mask attribute-map map-name`	Generates an aggregate with attributes specified in the route map.

See the "BGP Aggregate Route Examples" section at the end of this chapter for examples of using BGP aggregate routes.

Disabling Automatic Summarization of Network Numbers

In BGP Version 3, when a subnet is redistributed from an IGP into BGP, only the network route is injected into the BGP table. By default, this automatic summarization is enabled. To disable automatic network number summarization, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# no auto-summary`	Disables automatic network summarization.

Configuring BGP Community Filtering

BGP supports transit policies via controlled distribution of routing information. The distribution of routing information is based on one of the following three values:

- IP address (see the "Configuring BGP Route Filtering by Neighbor" section earlier in this chapter).
- The value of the autonomous system path attribute (see the "Configuring BGP Path Filtering by Neighbor" section earlier in this chapter).
- The value of the communities attribute (as described in this section).

The *communities* attribute is a way to group destinations into communities and apply routing decisions based on the communities. This method simplifies the configuration of a BGP speaker that controls distribution of routing information.

A *community* is a group of destinations that share some common attribute. Each destination can belong to multiple communities. Autonomous system administrators can define to which communities a destination belongs. By default, all destinations belong to the general Internet community. The community is carried as the communities attribute.

The communities attribute is an optional, transitive, global attribute in the numerical range from 1 to 4,294,967,200. Along with Internet community, there are a few predefined, well-known communities, as follows:

- internet—Advertise this route to the Internet community. All routers belong to it.
- no-export—Do not advertise this route to eBGP peers.
- no-advertise—Do not advertise this route to any peer (internal or external).
- local-as—Do not advertise this route to peers outside the local autonomous system. This route will not be advertised to other autonomous systems or sub-autonomous systems when confederations are configured.

Based on the community, you can control which routing information to accept, prefer, or distribute to other neighbors. A BGP speaker can set, append, or modify the community of a route when you learn, advertise, or redistribute routes. When routes are aggregated, the resulting aggregate has a communities attribute that contains all communities from all the initial routes.

You can use community lists to create groups of communities to use in a match clause of a route map. Just like an access list, a series of community lists can be created. Statements are checked until a match is found. As soon as one statement is satisfied, the test is concluded.

To create a community list, use the following command in global configuration mode:

Command	Purpose
Router(config)# **ip community-list** *community-list-number* {**permit** | **deny**} *community-number*	Creates a community list.

To set the communities attribute and match clauses based on communities, see the **match community-list** and **set community** route map configuration commands in the "Redistribute Routing Information" section in the "Configuring IP Routing Protocol-Independent Features" chapter.

By default, no communities attribute is sent to a neighbor. To specify that the communities attribute to be sent to the neighbor at an IP address, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]	Specifies that the communities attribute be sent to the neighbor at this IP address. Both standard and extended communities can be specified with the **both** keyword. Only standard or only extended can be specified with the **standard** and **extended** keywords.

To remove communities from the community attribute of an inbound or outbound update using a route map to filter and determine the communities to be deleted, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# **set comm-list** *community-list-number* **delete**`	Removes communities in a community attribute that match a standard or extended community list.

Specifying the Format for the Community

A BGP community is displayed in a two-part format 2 bytes long in the **show ip bgp community** EXEC command output, and wherever communities are displayed in the router configuration, such as router maps and community lists. In the most recent version of the RFC for BGP, a community is of the form AA:NN, where the first part is the autonomous system number and the second part is a 2-byte number. The Cisco default community format is in the format NNAA.

To display BGP communities in the new format, use the following command in global configuration mode:

Command	Purpose
`Router(config)# **ip bgp-community new-format**`	Displays and parses BGP communities in the format AA:NN.

Configuring BGP Conditional Advertisement

BGP advertises routes from its routing table to external peers (peers in different autonomous systems) by default. The BGP Conditional Advertisement feature provides additional control of route advertisement depending on the existence of other prefixes in the BGP table. Normally, routes are propagated regardless of the existence of a different path. The BGP Conditional Advertisement feature uses the non-exist-map and the advertise-map to track routes by the route prefix. If a route prefix is not present in the non-exist-map, the route specified by the advertise-map is announced. The announced route is installed to the BGP routing table as a locally originated route and will behave as a locally originated route. The announced route will be originated by BGP only if the corresponding IGP route exists. After the prefix is locally originated by BGP, BGP will advertise the prefix to internal and external peers. If the route prefix is present, the route in the advertise-map is not announced.

Conditional advertisement can be useful in a multihomed network, in which some prefixes are to be advertised to one of the providers, only if information from the other provider is missing. This condition would indicate a failure in the peering session, or partial reachability.

If the same information is advertised to all providers in a multihomed environment, the information is duplicated in the global BGP table. When the BGP Conditional Advertisement feature is used, only partial routes are advertised to each provider, and the size of the global BGP table is not increased with redundant information. The administrator can also guarantee the path that inbound traffic will follow because only specific paths are advertised to providers.

Note The conditional BGP announcements are sent in addition to the normal announcements that a BGP router sends to its peers.

Note Autonomous system path list information cannot be used for conditional advertisement because the IP routing table does not contain autonomous system path information.

BGP Conditional Advertisement Configuration Task List

See the following section for configuration tasks for the BGP Conditional Advertisement feature. Each task in the list indicates if the task is optional or required.

- Configure the route-maps that will be used in conjunction with the advertise-map and the non-exist-map. This step may include the configuration of access-lists and prefix-lists. (Required)
- Configure the router to run BGP. (Required)
- Configure the advertise-map and the non-exist-map with the **neighbor advertise-map non-exist-map** router configuration command. (Required)
- Verify that the BGP Condition Advertisement feature has been configured with the **show ip bgp neighbor** command. (Optional)

Conditional Advertisement of a Set of Routes

To conditionally advertise a set of routes, use the following commands beginning in router configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **`router bgp`** *`as-number`*	Configures the router to run a BGP process.
Step 2	`Router(config-router)#` **`neighbor`** *`ip-address`* **`remote-as`** *`as-number`*	Specifies the peer that should receive conditional advertisement for a given set routes.
Step 3	`Router(config-router)#` **`neighbor`** *`ip-address`* **`advertise-map`** *`map1`* **`non-exist-map`** *`map2`*	Configures the advertise-map and non-exist map for the BGP Conditional Advertisement feature.

See the "BGP Conditional Advertisement Configuration Examples" section at the end of this chapter for an example configuration of BGP conditional advertisement.

Verifying BGP Conditional Advertisement

To verify that the BGP Condition Advertisement feature has been configured, use the **show ip bgp neighbor** command. The **show ip bgp neighbor EXEC** command will show the status of the BGP Conditional Advertisement feature as initialized or uninitialized. The following example shows output from the **show ip bgp neighbor EXEC** command:

```
router# show ip bgp neigbor 172.16.1.1
BGP neighbor is 172.16.1.1,  remote AS 65200, internal link
 Description:link to boston as 65200
  BGP version 4, remote router ID 10.1.1.1
  BGP state = Established, up for 01:04:30
  Last read 00:00:30, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received
    Address family IPv4 Unicast:advertised and received
  Received 83 messages, 0 notifications, 0 in queue
  Sent 78 messages, 0 notifications, 0 in queue
 Route refresh request:received 0, sent 0
 Minimum time between advertisement runs is 5 seconds

For address family:IPv4 Unicast
 BGP table version 18, neighbor version 18
 Index 2, Offset 0, Mask 0x4
 Inbound soft reconfiguration allowed
 NEXT_HOP is always this router
 Community attribute sent to this neighbor
 Condition-map old-route, Advertise-map new-route, status:Uninitialized
 2 accepted prefixes consume 72 bytes
 Prefix advertised 7, suppressed 0, withdrawn 4

 Connections established 1; dropped 0
 Last reset 01:05:29, due to Soft reconfig change
```

BGP Conditional Advertisement Troubleshooting Tips

This section provides troubleshooting information for the BGP conditional advertisement feature.

The BGP Conditional Advertisement feature is based on the nonexistence of a prefix and the advertisement of another. Normally, only two problems can occur:

- The tracked prefix exists, but the conditional advertisement occurs.
- The tracked prefix does not exist, and the conditional advertisement does not occur.

The same method of troubleshooting is used for both problems:

- Verify the existence (or not) of the tracked prefix in the BGP table with the **show ip bgp EXEC** command.
- Verify the advertisement (or not) of the other prefix using the **show ip bgp neighbor advertised-routes EXEC** command.

The user needs to ensure that all of the characteristics specified in the route maps match the routes in the BGP table.

Configuring a Routing Domain Confederation

One way to reduce the iBGP mesh is to divide an autonomous system into multiple subautonomous systems and group them into a single confederation. To the outside world, the confederation looks like a single autonomous system. Each autonomous system is fully meshed within itself, and has a few connections to other autonomous systems in the same confederation. Even though the peers in different autonomous systems have eBGP sessions, they exchange routing information as if they were iBGP peers. Specifically, the next hop, MED, and local preference information is preserved. This feature allows the you to retain a single IGP for all of the autonomous systems.

To configure a BGP confederation, you must specify a confederation identifier. To the outside world, the group of autonomous systems will look like a single autonomous system with the confederation identifier as the autonomous system number. To configure a BGP confederation identifier, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# `**`bgp confederation identifier`**` `*`as-number`*	Configures a BGP confederation.

7487 3

In order to treat the neighbors from other autonomous systems within the confederation as special eBGP peers, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **bgp confederation peers** *as-number* [as-number]	Specifies the autonomous systems that belong to the confederation.

See the "BGP Community with Route Maps Examples" section at the end of this chapter for an example configuration of several peers in a confederation.

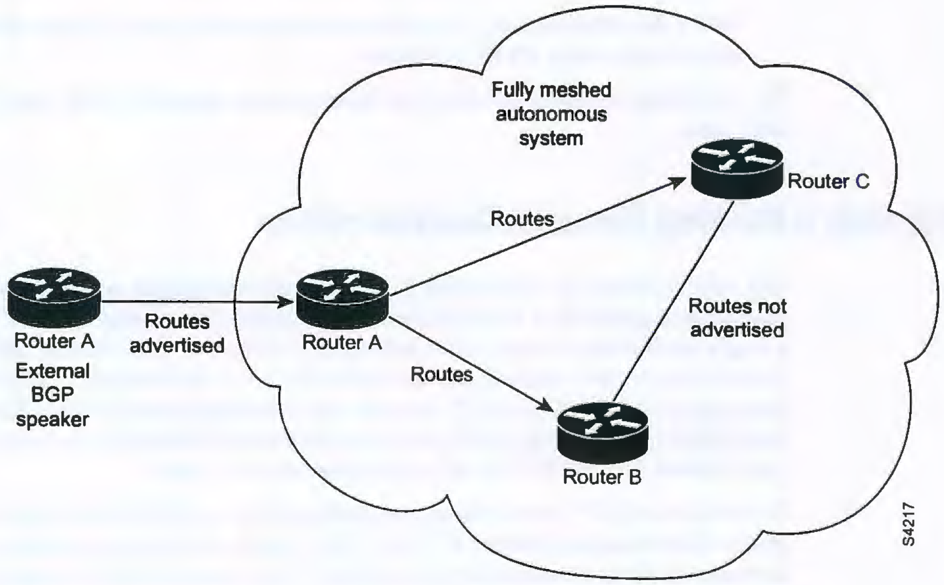
For an alternative way to reduce the iBGP mesh, see the next section, "Configuring a Route Reflector."

Configuring a Route Reflector

BGP requires that all iBGP speakers be fully meshed. However, this requirement does not scale well when there are many iBGP speakers. Instead of configuring a confederation, another way to reduce the iBGP mesh is to configure a *route reflector.*

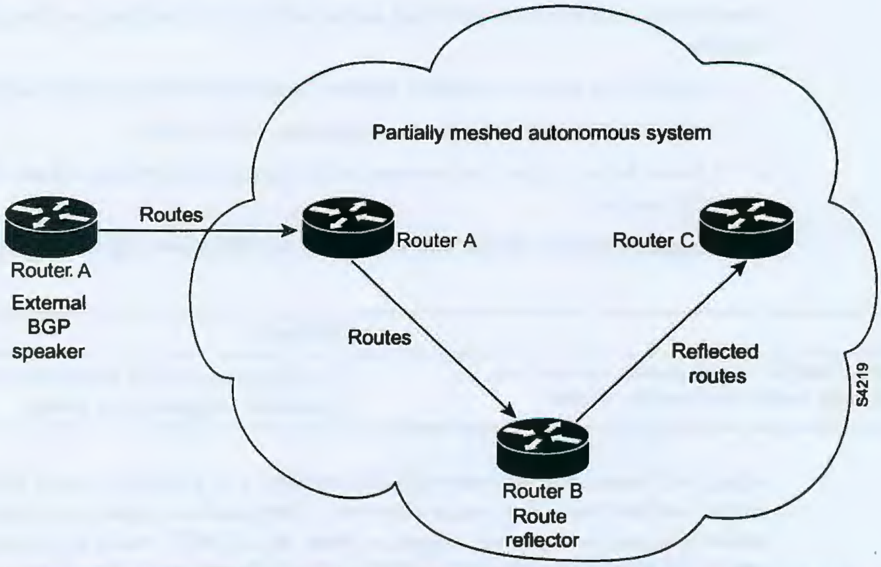
Figure 53 illustrates a simple iBGP configuration with three iBGP speakers (Routers A, B, and C). Without route reflectors, when Router A receives a route from an external neighbor, it must advertise it to both routers B and C. Routers B and C do not readvertise the iBGP learned route to other iBGP speakers because the routers do not pass on routes learned from internal neighbors to other internal neighbors, thus preventing a routing information loop.

Figure 53 Three Fully Meshed iBGP Speakers



With route reflectors, all iBGP speakers need not be fully meshed because there is a method to pass learned routes to neighbors. In this model, an iBGP peer is configured to be a route reflector responsible for passing iBGP learned routes to a set of iBGP neighbors. In Figure 54, Router B is configured as a route reflector. When the route reflector receives routes advertised from Router A, it advertises them to Router C, and vice versa. This scheme eliminates the need for the iBGP session between Routers A and C.

Figure 54 Simple BGP Model with a Route Reflector



The internal peers of the route reflector are divided into two groups: client peers and all the other routers in the autonomous system (nonclient peers). A route reflector reflects routes between these two groups. The route reflector and its client peers form a *cluster*. The nonclient peers must be fully meshed with each other, but the client peers need not be fully meshed. The clients in the cluster do not communicate with iBGP speakers outside their cluster.

Figure 55 More Complex BGP Route Reflector Model

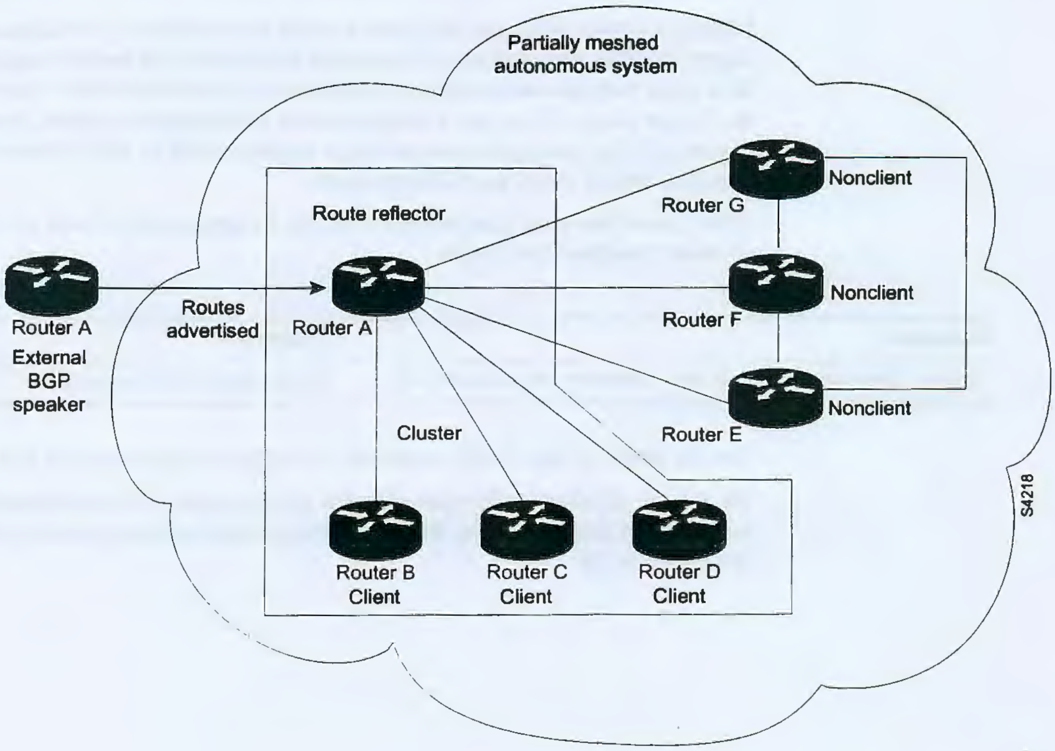


Figure 55 illustrates a more complex route reflector scheme. Router A is the route reflector in a cluster with routers B, C, and D. Routers E, F, and G are fully meshed, nonclient routers.

When the route reflector receives an advertised route, depending on the neighbor, it takes the following actions:

- A route from an external BGP speaker is advertised to all clients and nonclient peers.
- A route from a nonclient peer is advertised to all clients.
- A route from a client is advertised to all clients and nonclient peers. Hence, the clients need not be fully meshed.

To configure a route reflector and its clients, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor ip-address | peer-group-name route-reflector-client`	Configures the local router as a BGP route reflector and the specified neighbor as a client.

Along with route reflector-aware BGP speakers, it is possible to have BGP speakers that do not understand the concept of route reflectors. They can be members of either client or nonclient groups allowing a easy and gradual migration from the old BGP model to the route reflector model. Initially, you could create a single cluster with a route reflector and a few clients. All the other iBGP speakers could be nonclient peers to the route reflector and then more clusters could be created gradually.

An autonomous system can have multiple route reflectors. A route reflector treats other route reflectors just like other iBGP speakers. A route reflector can be configured to have other route reflectors in a client group or nonclient group. In a simple configuration, the backbone could be divided into many clusters. Each route reflector would be configured with other route reflectors as nonclient peers (thus, all the route reflectors will be fully meshed). The clients are configured to maintain iBGP sessions with only the route reflector in their cluster.

Usually a cluster of clients will have a single route reflector. In that case, the cluster is identified by the router ID of the route reflector. To increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster. All the route reflectors serving a cluster should be fully meshed and all of them should have identical sets of client and nonclient peers.

If the cluster has more than one route reflector, configure the cluster ID by using the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp cluster-id cluster-id`	Configures the cluster ID.

Use the **show ip bgp** EXEC command to display the originator ID and the cluster-list attributes.

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, the route reflector need not reflect routes to clients.

To disable client-to-client route reflection, use the **no bgp client-to-client reflection** command in router configuration mode:

Command	Purpose
`Router(config-router)# no bgp client-to-client reflection`	Disables client-to-client route reflection.

As the iBGP learned routes are reflected, routing information may loop. The route reflector model has the following mechanisms to avoid routing loops:

- Originator ID is an optional, nontransitive BGP attribute. It is a 4-byte attributed created by a route reflector. The attribute carries the router ID of the originator of the route in the local autonomous system. Therefore, if a misconfiguration causes routing information to come back to the originator, the information is ignored.
- Cluster-list is an optional, nontransitive BGP attribute. It is a sequence of cluster IDs that the route has passed. When a route reflector reflects a route from its clients to nonclient peers, and vice versa, it appends the local cluster ID to the cluster-list. If the cluster-list is empty, a new cluster-list is created. Using this attribute, a route reflector can identify if routing information is looped back to the same cluster due to misconfiguration. If the local cluster ID is found in the cluster-list, the advertisement is ignored.
- Use **set** clauses in outbound route maps to modify attributes, possibly creating routing loops. To avoid this behavior, **set** clauses of outbound route maps are ignored for routes reflected to iBGP peers.

Configuring BGP Peer Groups

Often, in a BGP speaker, many neighbors are configured with the same update policies (that is, the same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and, more importantly, to make updating more efficient. When you have many peers, this approach is highly recommended.

The three steps to configure a BGP peer group, described in the following sections, are as follows:

1. Creating the Peer Group
2. Assigning Options to the Peer Group
3. Making Neighbors Members of the Peer Group

You can disable a BGP peer or peer group without removing all the configuration information using the **neighbor shutdown** router configuration command.

Creating the Peer Group

To create a BGP peer group, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# neighbor peer-group-name peer-group`	Creates a BGP peer group.

Assigning Options to the Peer Group

After you create a peer group, you configure the peer group with **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members can also be configured to override the options that do not affect outbound updates.

Peer group members will always inherit the following attributes: minimum-advertisement-interval, next-hop-self, out-route-map, out-filter-list, out-dist-list, remote-as (if configured), version, and update-source. All the peer group members will inherit changes made to the peer group.

To assign configuration options to an individual neighbor, specify any of the following commands using the IP address. To assign the options to a peer group, specify any of the commands using the peer group name. Use the following commands in router configuration mode as needed.

Command	Purpose
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*	Specifies a BGP neighbor.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **description** *text*	Associates a description with a neighbor.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **send-community**	Specifies that the communities attribute be sent to the neighbor at this IP address.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface-type*	Allows iBGP sessions to use any operational interface for TCP connections.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop**	Allows BGP sessions, even when the neighbor is not on a directly connected segment. The multihop session is not established if the only route to the address of the multihop peer is the default route (0.0.0.0).
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*	Sets the minimum interval between sending BGP routing updates.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**]	Limits the number of prefixes allowed from a neighbor.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **password** *string*	Invokes MD5 authentication on a TCP connection to a BGP peer.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | access-list-*name*} {**in** | **out**}	Filters BGP routing updates to and from neighbors, as specified in an access list.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}	Establishes a BGP filter.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**	Disables next hop processing on the BGP updates to a neighbor.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **version** *value*	Specifies the BGP version to use when communicating with a neighbor.

Command	Purpose
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}	Applies a route map to incoming or outgoing routes.
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**	Configures the software to start storing received updates. This command requires at least one keyword. Currently the only keyword available is **inbound**, so the use of inbound is not optional.

If a peer group is not configured with a remote-as attribute, the members can be configured with the **neighbor remote-as** router configuration command. This command allows you to create peer groups containing eBGP neighbors.

You can customize inbound policies for peer group members (using, for example, a distribute list, route map, or filter list) because one identical copy of an update is sent to every member of a group. Therefore, neighbor options related to outgoing updates cannot be customized for peer group members.

External BGP peers normally must reside on a directly connected network. Sometimes it is useful to relax this restriction in order to test BGP; do so by specifying the **neighbor ebgp-multihop** router configuration command.

Note To avoid the accidental creation of loops through oscillating routes, the multihop session will not be established if the only route to the address of the multihop peer is the default route (0.0.0.0).

Members of a peer group can pass routes from one member of the peer group to another. For example, if router B is peering with routers A and C, router B can pass routes from router A to router C.

For iBGP, you might want to allow your BGP connections to stay up regardless of which interface is used to reach a neighbor. To enable this configuration, you first configure a *loopback* interface and assign it an IP address. Next, configure the BGP update source to be the loopback interface. Finally, configure your neighbor to use the address on the loopback interface. Now the iBGP session will be up as long as there is a route, regardless of any interface.

You can set the minimum interval of time between BGP routing updates.

You can invoke MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between them is verified. This feature must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. The authentication feature uses the MD5 algorithm. Invoking authentication causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection. If authentication is invoked and a segment fails authentication, then a message appears on the console.

See the "BGP Peer Group Examples" at the end of this chapter for an example of enabling MD5 authentication.

Making Neighbors Members of the Peer Group

To configure a BGP neighbor to be a member of a BGP peer group, use the following command in router configuration mode, using the same peer group name:

Command	Purpose
Router(config-router)# **neighbor** *ip-address* **peer-group** *peer-group-name*	Makes a BGP neighbor a member of the peer group.

See the “BGP Peer Group Examples” section at the end of this chapter for examples of iBGP and eBGP peer groups.

Disabling a Peer or Peer Group

To disable an existing BGP neighbor or neighbor peer group, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **neighbor** {*ip-address* | *peer-group-name*} **shutdown**	Shuts down or disables a BGP neighbor or peer group.

To enable a previously existing neighbor or neighbor peer group that had been disabled using the **neighbor shutdown** router configuration command, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **no neighbor** {*ip-address* | *peer-group-name*} **shutdown**	Enables a BGP neighbor or peer group.

Indicating Backdoor Routes

You can indicate which networks are reachable by using a *backdoor* route that the border router should use. A backdoor network is treated as a local network, except that it is not advertised. To configure backdoor routes, use the **network backdoor** command, beginning in router configuration mode:

Command	Purpose
Router(config-router)# **network** *ip-address* **backdoor**	Indicates reachable networks through backdoor routes.

Modifying Parameters While Updating the IP Routing Table

By default, when a BGP route is put into the IP routing table, the MED is converted to an IP route metric, the BGP next hop is used as the next hop for the IP route, and the tag is not set. However, you can use a route map to perform mapping. To modify metric and tag information when the IP routing table is updated with BGP learned routes, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **table-map** *map-name*	Applies a route map to routes when updating the IP routing table.

Setting Administrative Distance

Administrative distance is a measure of the preference of different routing protocols. BGP uses three different administrative distances: external, internal, and local. Routes learned through external BGP are given the external distance, routes learned with iBGP are given the internal distance, and routes that are part of this autonomous system are given the local distance. To assign a BGP administrative distance, use the following command in router configuration mode:

Command	Purpose

`Router(config-router)# `**`distance bgp`**
`external-distance internal-distance local-distance`
	Assigns a BGP administrative distance.

Changing the administrative distance of BGP routes is considered dangerous and generally is not recommended. The external distance should be lower than any other dynamic routing protocol, and the internal and local distances should be higher than any other dynamic routing protocol.

Adjusting BGP Timers

BGP uses certain timers to control periodic activities such as the sending of keepalive messages and the interval after not receiving a keepalive message after which the Cisco IOS software declares a peer dead. By default, the keepalive timer is 60 seconds, and the hold-time timer is 180 seconds.You can adjust these timers. When a connection is started, BGP will negotiate the hold time with the neighbor. The smaller of the two hold times will be chosen. The keepalive timer is then set based on the negotiated hold time and the configured keepalive time.

To adjust BGP timers for all neighbors, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# `**`timers bgp`**` `*`keepalive holdtime`*	Adjusts BGP timers for all neighbors.

To adjust BTP keepalive and hold-time timers for a specific neighbor, use the following command in router configuration mode:

Command	Purpose

`Router(config-router)# `**`neighbor`**` [`*`ip-address`*` |`
`peer-group-name``] `**`timers`**` `*`keepalive holdtime`*
	Sets the keepalive and hold-time timers (in seconds) for the specified peer or peer group.

Note The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the **timers bgp** router configuration command.

To clear the timers for a BGP neighbor or peer group, use the **no** form of the **neighbor timers** command.

7479
3

Changing the Default Local Preference Value

You can define a particular path as more preferable or less preferable than other paths by changing the default local preference value of 100. To assign a different default local preference value, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **bgp default local-preference** *value*	Changes the default local preference value.

You can use route maps to change the default local preference of specific paths. See the "BGP Route Map Examples" section at the end of this chapter for examples when used with BGP route maps.

Redistributing Network 0.0.0.0

By default, you are not allowed to redistribute network 0.0.0.0. To permit the redistribution of networ' 0.0.0.0, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **default-information originate**	Allows the redistribution of network 0.0.0.0 into BGP.

Configuring the Router to Consider a Missing MED as Worst Path

To configure the router to consider a path with a missing MED attribute as the worst path, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **bgp bestpath med missing-as-worst**	Configures the router to consider a missing MED as having a value of infinity, making the path without a MED value the least desirable path.

Selecting Path Based on MEDs from Other Autonomous Systems

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED.

By default, during the best path selection process, MED comparison is done only among paths from the same autonomous system. You can allow comparison of MEDs among paths regardless of the autonomous system from which the paths are received. To do so, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **bgp always-compare-med**	Allows the comparison of MEDs for paths from neighbors in different autonomous systems.

Configuring the Router to Use the MED to Choose a Path from Subautonomous System Paths

To configure the router to consider the MED value in choosing a path, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp bestpath med confed`	Configures the router to consider the MED in choosing a path from among those advertised by different subautonomous systems within a confederation.

The comparison between MEDs is only made if there are no external autonomous systems in the path (an external autonomous system is an autonomous system that is not within the confederation). If there is an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison is not made.

The following example compares route A with these paths:

```
path= 65000 65004, med=2
path= 65001 65004, med=3
path= 65002 65004, med=4
path= 65003 1, med=1
```

In this case, path 1 would be chosen if the **bgp bestpath med confed** router configuration command is enabled. The fourth path has a lower MED, but it is not involved in the MED comparison because there is an external autonomous system is in this path.

Configuring the Router to Use the MED to Choose a Path in a Confederation

To configure the router to use the MED to select the best path from among paths advertised by a single subautonomous system within a confederation, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp deterministic med`	Configures the router to compare the MED variable when choosing among routes advertised by different peers in the same autonomous system.

Note If the **bgp always-compare-med** router configuration command is enabled, all paths are fully comparable, including those from other autonomous systems in the confederation, even if the **bgp deterministic med** command is also enabled.

4477

Configuring Route Dampening

Route dampening is a BGP feature designed to minimize the propagation of flapping routes across an internetwork. A route is considered to be flapping when it is repeatedly available, then unavailable, then available, then unavailable, and so on.

For example, consider a network with three BGP autonomous systems: autonomous system 1, autonomous system 2, and autonomous system 3. Suppose the route to network A in autonomous system 1 flaps (it becomes unavailable). Under circumstances without route dampening, the eBGP neighbor of autonomous system 1 to autonomous system 2 sends a withdraw message to autonomous system 2. The border router in autonomous system 2, in turn, propagates the withdraw message to autonomous system 3. When the route to network A reappears, autonomous system 1 sends an advertisement message to autonomous system 2, which sends it to autonomous system 3. If the route to network A repeatedly becomes unavailable, then available, many withdrawal and advertisement messages are sent. This is a problem in an internetwork connected to the Internet because a route flap in the Internet backbone usually involves many routes.

Note No penalty is applied to a BGP peer reset when route dampening is enabled. Although the reset withdraws the route, no penalty is applied in this instance, even if route flap dampening is enabled.

Minimizing Flapping

The route dampening feature minimizes the flapping problem as follows. Suppose again that the route to network A flaps. The router in autonomous system 2 (where route dampening is enabled) assigns network A a penalty of 1000 and moves it to history state. The router in autonomous system 2 continues to advertise the status of the route to neighbors. The penalties are cumulative. When the route flaps so often that the penalty exceeds a configurable suppress limit, the router stops advertising the route to network A, regardless of how many times it flaps. Thus, the route is dampened.

The penalty placed on network A is decayed until the reuse limit is reached, upon which the route is once again advertised. At half of the reuse limit, the dampening information for the route to network A is removed.

Understanding Route Dampening Terms

The following terms are used when describing route dampening:

- Flap—A route is available, then unavailable, or vice versa.
- History state—After a route flaps once, it is assigned a penalty and put into history state, meaning the router does not have the best path, based on historical information.
- Penalty—Each time a route flaps, the router configured for route dampening in another autonomous system assigns the route a penalty of 1000. Penalties are cumulative. The penalty for the route is stored in the BGP routing table until the penalty exceeds the suppress limit. At that point, the route state changes from history to damp.
- Damp state—In this state, the route has flapped so often that the router will not advertise this route to BGP neighbors.
- Suppress limit—A route is suppressed when its penalty exceeds this limit. The default value is 2000.
- Half-life—Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds.

- Reuse limit—As the penalty for a flapping route decreases and falls below this reuse limit, the route is unsuppressed. That is, the route is added back to the BGP table and once again used for forwarding. The default reuse limit is 750. The process of unsuppressing routes occurs at 10-second increments. Every 10 seconds, the router finds out which routes are now unsuppressed and advertises them to the world.
- Maximum suppress limit—This value is the maximum amount of time a route can be suppressed. The default value is four times the half-life.

The routes external to an autonomous system learned via iBGP are not dampened. This policy prevent the iBGP peers from having a higher penalty for routes external to the autonomous system.

Enabling Route Dampening

To enable BGP route dampening, use the following command in address family or router configuration mode:

Command	Purpose
`Router(config)# bgp dampening`	Enables BGP route dampening.

To change the default values of various dampening factors, use the following command in address family or router configuration mode:

Command	Purpose
`Router(config)# bgp dampening half-life reuse suppress max-suppress [route-map map-name]`	Changes the default values of route dampening factors.

Monitoring and Maintaining BGP Route Dampening

You can monitor the flaps of all the paths that are flapping. The statistics will be deleted once the route is not suppressed and is stable for at least one half-life. To display flap statistics, use the following commands in EXEC mode as needed:

Command	Purpose
`Router# show ip bgp flap-statistics`	Displays BGP flap statistics for all paths.
`Router# show ip bgp flap-statistics regexp regexp`	Displays BGP flap statistics for all paths that match the regular expression.
`Router# show ip bgp flap-statistics filter-list access-list`	Displays BGP flap statistics for all paths that pass the filter.
`Router# show ip bgp flap-statistics ip-address mask`	Displays BGP flap statistics for a single entry.
`Router# show ip bgp flap-statistics ip-address mask longer-prefix`	Displays BGP flap statistics for more specific entries.

To clear BGP flap statistics (thus making it less likely that the route will be dampened), use the following commands in EXEC mode as needed:

Command	Purpose
Router# **clear ip bgp flap-statistics**	Clears BGP flap statistics for all routes.
Router# **clear ip bgp flap-statistics regexp** *regexp*	Clears BGP flap statistics for all paths that match the regular expression.
Router# **clear ip bgp flap-statistics filter-list** *list*	Clears BGP flap statistics for all paths that pass the filter.
Router# **clear ip bgp flap-statistics** *ip-address mask*	Clears BGP flap statistics for a single entry.
Router# **clear ip bgp** *ip-address* **flap-statistics**	Clears BGP flap statistics for all paths from a neighbor.

Note The flap statistics for a route are also cleared when a BGP peer is reset. Although the reset withdraws the route, there is no penalty applied in this instance, even if route flap dampening is enabled.

Once a route is dampened, you can display BGP route dampening information, including the time remaining before the dampened routes will be unsuppressed. To display the information, use the following command in EXEC mode:

Command	Purpose
Router# **show ip bgp dampened-paths**	Displays the dampened routes, including the time remaining before they will be unsuppressed.

You can clear BGP route dampening information and unsuppress any suppressed routes by using the following command in EXEC mode:

Command	Purpose
Router# **clear ip bgp dampening** [*ip-address network-mask*]	Clears route dampening information and unsuppresses the suppressed routes.

Monitoring and Maintaining BGP

You can remove all contents of a particular cache, table, or database. You also can display specific statistics. The following sections describe each of these tasks.

Clearing Caches, Tables, and Databases

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database can become necessary when the contents of the particular structure have become, or are suspected to be, invalid.

To clear caches, tables, and databases for BGP, use the following commands in EXEC mode, as needed:

Command	Purpose
Router# **clear ip bgp** *neighbor-address*	Resets a particular BGP connection.
Router# **clear ip bgp** *	Resets all BGP connections.
Router# **clear ip bgp peer-group** *tag*	Removes all members of a BGP peer group.

Displaying System and Network Statistics

You can display specific statistics such as the contents of BGP routing tables, caches, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path that the packets of your device are taking through the network.

To display various routing statistics, use the following commands in EXEC mode, as needed:

Command	Purpose
Router# **show ip bgp** *prefix*	Displays peer groups and peers not in peer groups to which the prefix has been advertised. Also displays prefix attributes such as the next hop and the local prefix.
Router# **show ip bgp cidr-only**	Displays all BGP routes that contain subnet and supernet network masks.
Router# **show ip bgp community** *community-number* [**exact**]	Displays routes that belong to the specified communities.
Router# **show ip bgp community-list** *community-list-number* [**exact**]	Displays routes that are permitted by the community list.
Router# **show ip bgp filter-list** *access-list-number*	Displays routes that are matched by the specified autonomous system path access list.
Router# **show ip bgp inconsistent-as**	Displays the routes with inconsistent originating autonomous systems.
Router# **show ip bgp regexp** *regexp*	Displays the routes that have an autonomous system path that matches the specified regular expression entered on the command line.
Router# **show ip bgp**	Displays the contents of the BGP routing table.
Router# **show ip bgp neighbors** [*neighbor-address*]	Displays detailed information on the BGP and TCP connections to individual neighbors.
Router# **show ip bgp neighbors** [*address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes**]	Displays routes learned from a particular BGP neighbor.
Router# **show ip bgp paths**	Displays all BGP paths in the database.
Router# **show ip bgp peer-group** [*tag*] [**summary**]	Displays information about BGP peer groups.
Router# **show ip bgp summary**	Displays the status of all BGP connections.

Logging Changes in Neighbor Status

To enable the logging of messages generated when a BGP neighbor resets, comes up, or goes down, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# bgp log-neighbor-changes`	Logs messages generated when a BGP neighbor goes up or down, or resets

BGP Configuration Examples

The following sections provide BGP configuration examples:

- BGP Route Map Examples
- BGP Neighbor Configuration Examples
- BGP Prefix List Filtering Examples
- BGP Soft Reset Examples
- BGP Synchronization Examples
- BGP Path Filtering by Neighbor Examples
- BGP Aggregate Route Examples
- BGP Community with Route Maps Examples
- BGP Conditional Advertisement Configuration Examples
- BGP Confederation Examples
- BGP Peer Group Examples
- TCP MD5 Authentication for BGP Examples

BGP Route Map Examples

The following example shows how you can use route maps to modify incoming data from a neighbor. Any route received from 140.222.1.1 that matches the filter parameters set in autonomous system access list 200 will have its weight set to 200 and its local preference set to 250, and it will be accepted.

```
router bgp 100
!
 neighbor 140.222.1.1 route-map FIX-WEIGHT in
 neighbor 140.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800
!
route-map FIX-WEIGHT permit 10
 match as-path 200
 set local-preference 250
 set weight200
```

In the following example, the route map named freddy marks all paths originating from autonomous system 690 with an MED metric attribute of 127. The second permit clause is required so that routes not matching autonomous system path list 1 will still be sent to neighbor 1.1.1.1.

```
router bgp 100
 neighbor 1.1.1.1 route-map freddy out
!
ip as-path access-list 1 permit ^690_
ip as-path access-list 2 permit .*
!
route-map freddy permit 10
 match as-path 1
 set metric 127
!
route-map freddy permit 20
 match as-path 2
```

The following example shows how you can use route maps to modify redistributed information from the IP forwarding table:

```
router bgp 100
 redistribute igrp 109 route-map igrp2bgp
!
route-map igrp2bgp
 match ip address 1
 set local-preference 25
 set metric 127
 set weight 30000
 set next-hop 192.92.68.24
 set origin igp
!
access-list 1 permit 131.108.0.0 0.0.255.255
access-list 1 permit 160.89.0.0 0.0.255.255
access-list 1 permit 198.112.0.0 0.0.127.255
```

It is proper behavior to not accept any autonomous system path not matching the **match** clause of the route map. This behavior means that you will not set the metric and the Cisco IOS software will not accept the route. However, you can configure the software to accept autonomous system paths not matched in the **match** clause of the **route-map** router configuration command by using multiple maps of the same name, some without accompanying **set** commands.

```
route-map fnord permit 10
 match as-path 1
 set local-preference 5
!
route-map fnord permit 20
 match as-path 2
```

The following example shows how you can use route maps in a reverse operation to set the route tag (as defined by the BGP/OSPF interaction document, RFC 1403) when exporting routes from BGP into the main IP routing table:

```
router bgp 100
 table-map set_ospf_tag
!
route-map set_ospf_tag
 match as-path 1
 set automatic-tag
!
ip as-path access-list 1 permit .*
```

The following example shows how the route map named set-as-path is applied to outbound updates to the neighbor 200.69.232.70. The route map will prepend the autonomous system path "100 100" to routes that pass access list 1. The second part of the route map is to permit the advertisement of other routes.

```
router bgp 100
 network 171.60.0.0
 network 172.60.0.0
 neighbor 200.69.232.70 remote-as 200
 neighbor 200.69.232.70 route-map set-as-path out
!
route-map set-as-path 10 permit
 match address 1
 set as-path prepend 100 100
!
route-map set-as-path 20 permit
 match address 2
!
access-list 1 permit 171.60.0.0 0.0.255.255
access-list 1 permit 172.60.0.0 0.0.255.255
!
access-list 2 permit 0.0.0.0 255.255.255.255
```

Inbound route maps could perform prefix-based matching and set various parameters of the update. Inbound prefix matching is available in addition to autonomous system path and community list matching. The following example shows how the **set local-preference** route-map configuration command sets the local preference of the inbound prefix 140.10.0.0/16 to 120:

```
!
router bgp 100
 network 131.108.0.0
 neighbor 131.108.1.1 remote-as 200
 neighbor 131.108.1.1 route-map set-local-pref in
!
route-map set-local-pref permit 10
 match ip address 2
 set local preference 120
!
route-map set-local-pref permit 20
!
access-list 2 permit 140.10.0.0 0.0.255.255
access-list 2 deny any
```

The following examples show how to ensure that traffic from one router on a shared LAN will always be passed through a second router, rather than being sent directly to a third router on the same LAN.

Routers A, B, and C connect to the same LAN. Router A peers with router B, and router B peers with router C. Router B sends traffic over the routes of router A to router C, but wants to make sure that all traffic from router C to router A goes through router B, rather than directly from router C to router A over the shared LAN. This configuration can be useful for traffic accounting purposes or to satisfy the peering agreement between router C and router B. You can achieve this configuration by using the **set ip next-hop** route-map configuration command as shown in the following two examples.

Example one applies an inbound route map on the BGP session of router C with router B.

Router A Configuration

```
router bgp 100
 neighbor 1.1.1.2 remote-as 200
```

Router B Configuration

```
router bgp 200
```

```
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.3 remote-as 300
```

Router C Configuration

```
router bgp 300
 neighbor 1.1.1.2 remote-as 200
 neighbor 1.1.1.2 route-map set-peer-address in

route-map set-peer-address permit 10
 set ip next-hop peer-address
```

The following example applies an outbound route map on the BGP session of router B with router C:

Router A Configuration

```
router bgp 100
 neighbor 1.1.1.2 remote-as 200
```

Router B Configuration

```
router bgp 200
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.3 remote-as 300
 neighbor 1.1.1.3 route-map set-peer-address out

route-map set-peer-address permit 10
 set ip next-hop peer-address
```

Router C Configuration

```
router bgp 300
 neighbor 1.1.1.2 remote-as 200
```

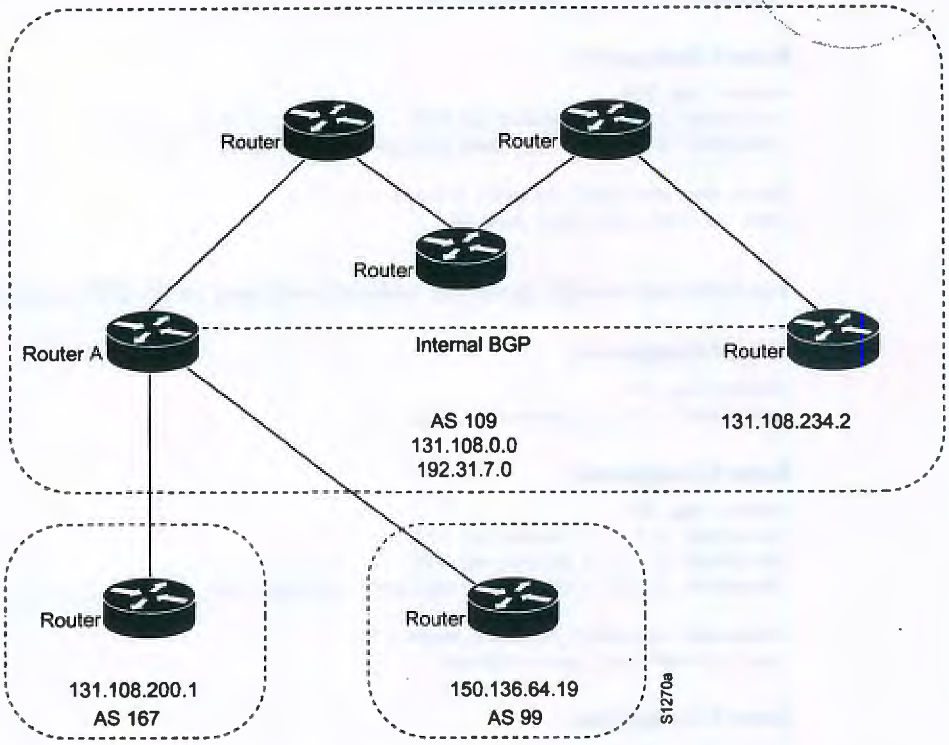
BGP Neighbor Configuration Examples

The following example shows how BGP neighbors on an autonomous system are configured to share information. In the example, a BGP router is assigned to autonomous system 109, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 131.108.0.0 and 192.31.7.0 with the neighbor routers. The first router listed is in a different autonomous system; the second **neighbor remote-as** router configuration command specifies an internal neighbor (with the same autonomous system number) at address 131.108.234.2; and the third **neighbor remote-as** router configuration command specifies a neighbor on a different autonomous system.

```
router bgp 109
 network 131.108.0.0
 network 192.31.7.0
 neighbor 131.108.200.1 remote-as 167
 neighbor 131.108.234.2 remote-as 109
 neighbor 150.136.64.19 remote-as 99
```

In Figure 56, Router A is being configured. The iBGP neighbor is not directly linked to Router A. External neighbors (in autonomous system 167 and autonomous system 99) must be linked directly to Router A.

Figure 56 Assigning Internal and External BGP Neighbors



BGP Prefix List Filtering Examples

The following examples show route filtering using a single prefix list and a group of prefixes, and how to add or delete an individual entry from a prefix list.

Route Filtering Configuration Example Using a Single Prefix List

The following example shows how a prefix list denies the default route 0.0.0.0/0:

```
ip prefix-list abc deny 0.0.0.0/0
```

The following example shows how a prefix list permits a route that matches the prefix 35.0.0.0/8:

```
ip prefix-list abc permit 35.0.0.0/8
```

The following example shows how to configure the BGP process so that it only accept prefixes with a prefix length of /8 to /24:

```
router bgp
version 2
network 101.20.20.0
distribute-list prefix max24 in
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

The following example configuration shows how to conditionally originate a default route (0.0.0.0/0) in RIP when a prefix 10.1.1.0/24 exists in the routing table:

```
ip prefix-list cond permit 10.1.1.0/24
!
route-map default-condition permit 10
match ip address prefix-list cond
!
router rip
default-information originate route-map default-condition
```

The following example shows how to configure BGP to accept routing updates from 192.1.1.1 only, besides filtering on the prefix length:

```
router bgp
distribute-list prefix max24 gateway allowlist in
!
ip prefix-list allowlist seq 5 permit 192.1.1.1/32
!
```

The following example shows how to direct the BGP process to filter incoming updates to the prefix using name1, and match the gateway (next hop) of the prefix being updated to the prefix list name2, on the Ethernet interface 0:

```
router bgp 103
distribute-list prefix name1 gateway name2 in ethernet 0.
```

Route Filtering Configuration Example Specifying a Group of Prefixes

The following example shows how to configure BGP to permit routes with a prefix length up to 24 in network 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

The following example shows how to configure BGP to deny routes with a prefix length greater than in 25 in 192/8:

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

The following example shows how to configure BGP to permit routes with a prefix length greater than 8 and less than 24 in all address space:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example shows how to configure BGP to deny routes with a prefix length greater than 25 in all address space:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

The following example shows how to configure BGP to deny all routes in 10/8, because any route in the Class A network 10.0.0.0/8 is denied if its mask is less than or equal to 32 bits:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

The following example shows how to configure BGP to deny routes with a mask greater than 25 in 204.70.1/24:

```
ip prefix-list abc deny 204.70.1.0/24 ge 25
```

The following example shows how to configure BGP to permit all routes:

```
ip prefix-list abc permit 0.0.0.0/0 le 32
```

Added or Deleted Prefix List Entries Examples

You can add or delete individual entries in a prefix list if a prefix list has the following initial configuration:

```
ip prefix-list abc deny 0.0.0.0/0 le 7
ip prefix-list abc deny 0.0.0.0/0 ge 25
ip prefix-list abc permit 35.0.0.0/8
ip prefix-list abc permit 204.70.0.0/15
```

The following example shows how to delete an entry from the prefix list so that 204.70.0.0 is not permitted, and add a new entry that permits 198.0.0.0/8:

```
no ip prefix-list abc permit 204.70.0.0/15
ip prefix-list abc permit 198.0.0.0/8
```

The new configuration is as follows:

```
ip prefix-list abc deny 0.0.0.0/0 le 7
ip prefix-list abc deny 0.0.0.0/0 ge 25
ip prefix-list abc permit 35.0.0.0/8
ip prefix-list abc permit 198.0.0.0/8
```

BGP Soft Reset Examples

The following examples show two ways to reset the connection for BGP peer 131.108.1.1.

Dynamic Inbound Soft Reset Example

The following examples shows the **clear ip bgp 131.108.1.1 soft in** EXEC command used to initiate a dynamic soft reconfiguration in the BGP peer 131.108.1.1. This command requires that the peer support the route refresh capability.

```
clear ip bgp 131.108.1.1 soft in
```

Inbound Soft Reset Using Stored Information Example

The following example shows how to enable inbound soft reconfiguration for the neighbor 131.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is performed later, the stored information will be used to generate a new set of inbound updates.

```
router bgp 100
 neighbor 131.108.1.1 remote-as 200
 neighbor 131.108.1.1 soft-reconfiguration inbound
```

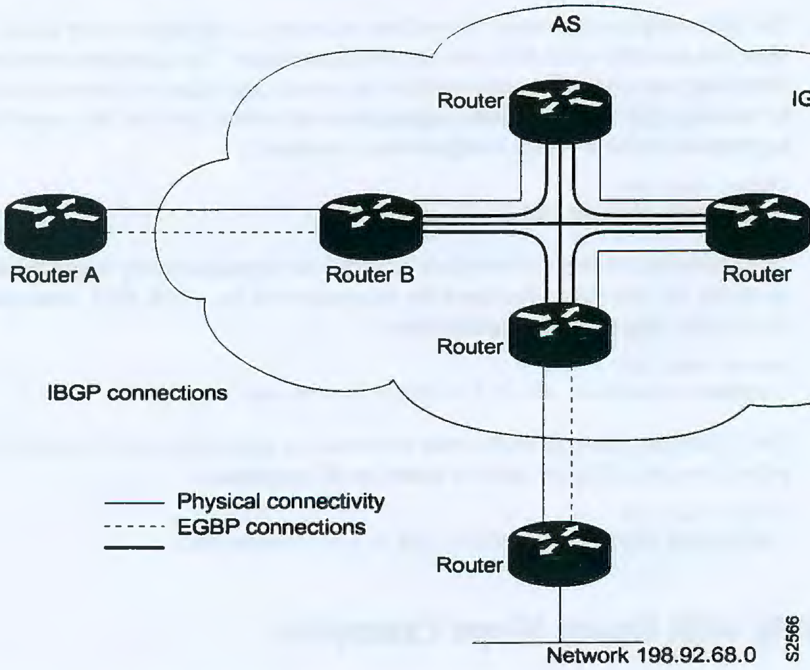
The following example clears the session with the neighbor 131.108.1.1.

```
clear ip bgp 131.108.1.1 soft in
```

BGP Synchronization Examples

The example shown in Figure 57 shows how to use the **no synchronization** router configuration command. In the figure, synchronization is on, and Router B does not advertise network 198.92.68.0 to Router A until an IGRP route for network 198.92.68.0 exists. If you specify the **no synchronization** router configuration command, Router B advertises network 198.92.68.0 as soon as possible. However, because routing information still must be sent to interior peers, you must configure a full iBGP mesh.

Figure 57 BGP Synchronization Configuration



BGP Path Filtering by Neighbor Examples

The following example shows BGP path filtering by neighbor. Only the routes that pass autonomous system path access list 2 will be sent to 193.1.12.10. Similarly, only routes passing access list 3 will be accepted from 193.1.12.10.

```
router bgp 200
 neighbor 193.1.12.10 remote-as 100
 neighbor 193.1.12.10 filter-list 1 out
 neighbor 193.1.12.10 filter-list 2 in
ip as-path access-list 1 permit _109_
ip as-path access-list 2 permit _200$
ip as-path access-list 2 permit ^100$
ip as-path access-list 3 deny _690$
ip as-path access-list 3 permit .*
```

BGP Aggregate Route Examples

The following examples show how you can use aggregate routes in BGP either by redistributing an aggregate route into BGP or by using the BGP Conditional Aggregate routing feature.

In the following example, the **redistribute static** router configuration command is used to redistribute aggregate route 193.0.0.0:

```
ip route 193.0.0.0 255.0.0.0 null 0
!
router bgp 100
 redistribute static
```

The following configuration shows how to create an aggregate entry in the BGP routing table when at least one specific route falls into the specified range. The aggregate route will be advertised as coming from your autonomous system and has the atomic aggregate attribute set to show that information might be missing. (By default, atomic aggregate is set unless you use the **as-set** keyword in the **aggregate-address** router configuration command.)

```
router bgp 100
 aggregate-address 193.0.0.0 255.0.0.0
```

The following example shows how to create an aggregate entry using the same rules as in the previous example, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized:

```
router bgp 100
 aggregate-address 193.0.0.0 255.0.0.0 as-set
```

The following example shows how to create the aggregate route for 193.0.0.0 and also suppress advertisements of more specific routes to all neighbors:

```
router bgp 100
 aggregate-address 193.0.0.0 255.0.0.0 summary-only
```

BGP Community with Route Maps Examples

This section contains three examples of the use of BGP communities with route maps, and two examples that also contain confederation configurations. For an example of how to configure a BGP confederation, see the section "BGP Confederation Examples" in this chapter.

The first example shows how the route map named set-community is applied to the outbound updates to the neighbor 171.69.232.50. The routes that pass access list 1 have the special community attribute value no-export. The remaining routes are advertised normally. This special community value automatically prevents the advertisement of those routes by the BGP speakers in autonomous system 200.

```
router bgp 100
 neighbor 171.69.232.50 remote-as 200
 neighbor 171.69.232.50 send-community
 neighbor 171.69.232.50 route-map set-community out
!
route-map set-community 10 permit
 match address 1
 set community no-export
!
route-map set-community 20 permit
 match address 2
```

The second example shows how the route map named set-community is applied to the outbound updates to neighbor 171.69.232.90. All the routes that originate from autonomous system 70 have the community values 200 200 added to their already existing values. All other routes are advertised as normal.

```
route-map bgp 200
 neighbor 171.69.232.90 remote-as 100
 neighbor 171.69.232.90 send-community
 neighbor 171.69.232.90 route-map set-community out
!
route-map set-community 10 permit
 match as-path 1
 set community 200 200 additive
!
route-map set-community 20 permit
!
ip as-path access-list 1 permit 70$
ip as-path access-list 2 permit .*
```

The third example shows how community-based matching is used to selectively set MED and local preference for routes from neighbor 171.69.232.55. All the routes that match community list 1 get the MED set to 8000, including any routes that have the communities 100 200 300 or 900 901. These routes could have other community values also.

All the routes that pass community list 2 get the local preference set to 500. This includes the routes that have community values 88 or 90. If they belong to any other community, they will not be matched by community list 2.

All the routes that match community list 3 get the local preference set to 50. Community list 3 will match all the routes because all the routes are members of the Internet community. Thus, all the remaining routes from neighbor 171.69.232.55 get a local preference 50.

```
router bgp 200
 neighbor 171.69.232.55 remote-as 100
 neighbor 171.69.232.55 route-map filter-on-community in
!
route-map filter-on-community 10 permit
 match community 1
 set metric 8000
!
route-map filter-on-community 20 permit
 match community 2 exact-match
 set local-preference 500
!
route-map filter-on-community 30 permit
 match community 3
 set local-preference 50
!
ip community-list 1 permit 100 200 300
ip community-list 1 permit 900 901
!
ip community-list 2 permit 88
ip community-list 2 permit 90
!
ip community-list 3 permit internet
```

The next two examples show how BGP community attributes are used with BGP confederation configurations to filter routes.

The next example shows how the route map named set-community is applied to the outbound updates to neighbor 171.69.232.50 and the local-as community attribute is used to filter the routes. The routes that pass access list 1 have the special community attribute value local-as. The remaining routes are advertised normally. This special community value automatically prevents the advertisement of those routes by the BGP speakers outside autonomous system 200.

```
router bgp 65000
 network 1.0.0.0 route-map set-community
 bgp confederation identifier 200
 bgp confederation peers 65001
 neighbor 171.69.232.50 remote-as 100
 neighbor 171.69.233.2 remote-as 65001
!
route-map set-community permit 10
 match ip address 1
 set community local-as
!
```

The following example shows how to use the local-as community attribute to filter the routes. Confederation 100 contains three autonomous systems: 100, 200, and 300. For network 1.0.0.0, the route map named set-local-as specifies that the advertised routes have the community attribute local-as. These routes are not advertised to any eBGP peer outside the local autonomous system. For network 2.0.0.0 the route map named set-no-export specifies that the routes advertised have the community attribute no-export.

A route between router 6500 and router 65001 does not cross the boundary between autonomous systems within the confederation. A route between subautonomous systems for which router 65000 is the controlling router does not cross the boundary between the confederation and an external autonomous system, and also does not cross the boundary between subautonomous systems within the local autonomous system. A route to from router 65000 to router 65001 would not be acceptable for network 1.0.0.0 because it crosses the boundary between subautonomous systems within the confederation.

```
router bgp 65001
 bgp confederation identifier 200
 bgp confederation peer 65000
 network 2.0.0.0 route-map  set-community
 neighbor 171.69.233.1 remote-as 65000
route-map set-community permit 10
 set community no-export
```

BGP Conditional Advertisement Configuration Examples

This section provides a configuration example of the BGP Conditional Advertisement feature. In the following example, the *ip-address* argument refers to the IP address of the neighbor, and the *map1-name* and *map2-name* arguments, refer to the names of the route maps:

neighbor{*ip-address*} **advertise-map** {*map1-name*} **non-exist-map** {*map2-name*}

no neighbor{*ip-address*} **advertise-map** {*map1-name*} **non-exist-map** {*map2-name*}

The route map associated with the non-exist-map specifies the prefix that the BGP speaker tracks. The route map associated with the advertise map specifies the prefix that is advertised when the prefix in the non-exist-map no longer exists. The prefix tracked by the BGP speaker must be present in the IP routing table for the conditional advertisement not to take place. In the following example, the router advertises 172.16.0.0/16 to its neighbor only if 192.168.7.0/24 is not present in the IP routing table.

To conditionally advertise a set of routes, use the following commands in router configuration mode:

```
router bgp 109
```

```
neighbor 10.89.2.33 remote-as 2051
neighbor 10.89.2.33 advertise-map map1-name non-exist-map map2-name
route-map map1-name permit 10
match ip address 1
route-map map2-name permit 10
match ip address 2
access-list 1 permit 172.16.0.0
access-list 2 permit 192.168.7.0
```

BGP Confederation Examples

The following is a sample configuration that shows several peers in a confederation. The confederation consists of three internal autonomous systems with autonomous system numbers 6001, 6002, and 6003. To the BGP speakers outside the confederation, the confederation looks like a normal autonomous system with autonomous system number 666 (specified via the **bgp confederation identifier** router configuration command).

In a BGP speaker in autonomous system 6001, the **bgp confederation peers** router configuration command marks the peers from autonomous systems 6002 and 6003 as special eBGP peers. Hence peers 171.69.232.55 and 171.69.232.56 will get the local preference, next hop, and MED unmodified in the updates. The router at 160.69.69.1 is a normal eBGP speaker and the updates received by it from this peer will be just like a normal eBGP update from a peer in autonomous system 666.

```
router bgp 6001
 bgp confederation identifier 666
 bgp confederation peers 6002 6003
 neighbor 171.69.232.55 remote-as 6002
 neighbor 171.69.232.56 remote-as 6003
 neighbor 160.69.69.1 remote-as 777
```

In a BGP speaker in autonomous system 6002, the peers from autonomous systems 6001 and 6003 are configured as special eBGP peers. 170.70.70.1 is a normal iBGP peer and 199.99.99.2 is a normal eBGP peer from autonomous system 700.

```
router bgp 6002
 bgp confederation identifier 666
 bgp confederation peers 6001 6003
 neighbor 170.70.70.1 remote-as 6002
 neighbor 171.69.232.57 remote-as 6001
 neighbor 171.69.232.56 remote-as 6003
 neighbor 199.99.99.2 remote-as 700
```

In a BGP speaker in autonomous system 6003, the peers from autonomous systems 6001 and 6002 are configured as special eBGP peers. 200.200.200.200 is a normal eBGP peer from autonomous system 701.

```
router bgp 6003
 bgp confederation identifier 666
 bgp confederation peers 6001 6002
 neighbor 171.69.232.57 remote-as 6001
 neighbor 171.69.232.55 remote-as 6002
 neighbor 200.200.200.200 remote-as 701
```

The following is a part of the configuration from the BGP speaker 200.200.200.205 from autonomous system 701 in the same example. Neighbor 171.69.232.56 is configured as a normal eBGP speaker from autonomous system 666. The internal division of the autonomous system into multiple autonomous systems is not known to the peers external to the confederation.

```
router bgp 701
 neighbor 171.69.232.56 remote-as 666
 neighbor 200.200.200.205 remote-as 701
```

For examples of how the BGP **set-community** route-map configuration command can be used with a confederation configuration, see the last two examples in the section"BGP Community with Route Maps Examples" in this chapter.

BGP Peer Group Examples

This section contains an iBGP peer group example and an eBGP peer group example.

iBGP Peer Group Example

The following example shows how the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the **router bgp** global configuration command and the **neighbor remote-as** router configuration command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The example also shows that, except for the neighbor at address 171.69.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 171.69.232.53 peer-group internal
 neighbor 171.69.232.54 peer-group internal
 neighbor 171.69.232.55 peer-group internal
 neighbor 171.69.232.55 filter-list 3 in
```

eBGP Peer Group Example

The following example shows how the peer group named external-peers is defined without the **neighbor remote-as** router configuration command, making it an eBGP peer group. Each member of the peer group is configured with its respective autonomous system number separately. Thus, the peer group consists of members from autonomous systems 200, 300, and 400. All the peer group members have set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 171.69.232.110, all have 101 as the inbound filter list.

```
router bgp 100
 neighbor external-peers peer-group
 neighbor external-peers route-map set-metric out
 neighbor external-peers filter-list 99 out
 neighbor external-peers filter-list 101 in
 neighbor 171.69.232.90 remote-as 200
 neighbor 171.69.232.90 peer-group external-peers
 neighbor 171.69.232.100 remote-as 300
 neighbor 171.69.232.100 peer-group external-peers
 neighbor 171.69.232.110 remote-as 400
 neighbor 171.69.232.110 peer-group external-peers
 neighbor 171.69.232.110 filter-list 400 in
```

TCP MD5 Authentication for BGP Examples

The following example specifies that the router and its BGP peer at 145.2.2.2 invoke MD5 authentication on the TCP connection between them:

```
router bgp 109
 neighbor 145.2.2.2 password v61ne0qkel33&
```

AP · GL

Configuring DVMRP Interoperability

This chapter describes the Distance Vector Multicast Routing Protocol (DVMRP) Interoperability feature. For a complete description of the DVMRP commands in this chapter, refer to the "IP Multicast Routing Commands" chapter of the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast* publication. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

Cisco routers run Protocol Independent Multicast (PIM), and know enough about DVMRP to successfully forward multicast packets to and receive packets from a DVMRP neighbor. It is also possible to propagate DVMRP routes into and through a PIM cloud. The Cisco IOS software propagates DVMRP routes and builds a separate database for these routes on each router, but PIM uses this routing information to make the packet-forwarding decision. Cisco IOS software does not implement the complete DVMRP.

DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths. Forwarding occurs until prune messages are received on those parent-child links, which further constrains the broadcast of multicast packets.

DVMRP is implemented in the equipment of many vendors and is based on the public-domain mrouted program. The Cisco IOS software supports dynamic discovery of DVMRP routers and can interoperate with them over traditional media such as Ethernet and FDDI, or over DVMRP-specific tunnels.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter.

Basic DVMRP Interoperability Configuration Task List

To configure basic interoperability with DVMRP machines, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional.

- Configuring DVMRP Interoperability (Required)
- Configuring a DVMRP Tunnel (Optional)
- Advertising Network 0.0.0.0 to DVMRP Neighbors (Optional)

For more advanced DVMRP interoperability features, see the section "Advanced DVMRP Interoperability Configuration Task List" later in this chapter.

Configuring DVMRP Interoperability

Cisco multicast routers using PIM can interoperate with non-Cisco multicast routers that use the DVMRP.

PIM routers dynamically discover DVMRP multicast routers on attached networks. Once a DVMRP neighbor has been discovered, the router periodically sends DVMRP report messages advertising the unicast sources reachable in the PIM domain. By default, directly connected subnets and networks are advertised. The router forwards multicast packets that have been forwarded by DVMRP routers and, in turn, forwards multicast packets to DVMRP routers.

You can configure which sources are advertised and which metrics are used by configuring the **ip dvmrp metric** interface configuration command. You can also direct all sources learned via a particular unicast routing process to be advertised into DVMRP.

The mrouted protocol is a public-domain implementation of DVMRP. It is necessary to use mrouted Version 3.8 (which implements a nonpruning version of DVMRP) when Cisco routers are directly connected to DVMRP routers or interoperate with DVMRP routers over an multicast backbone (MBONE) tunnel. DVMRP advertisements produced by the Cisco IOS software can cause older versions of mrouted to corrupt their routing tables and those of their neighbors. Any router connected to the MBONE should have an access list to limit the number of unicast routes that are advertised via DVM.

To configure the sources that are advertised and the metrics that are used when DVMRP report messages are sent, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **`ip dvmrp metric`** *`metric`* `[`**`list`** *`access-list`*`] [`*`protocol process-id`*`]`	Configures the metric associated with a set of destinations for DVMRP reports.

A more sophisticated way to achieve the same results as the preceding command is to use a route map instead of an access list. Thus, you have a finer granularity of control. To subject unicast routes to route map conditions before they are injected into DVMRP, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)#` **`ip dvmrp metric`** *`metric`* `[`**`route-map`** *`map-name`*`]`	Subjects unicast routes to route map conditions before they are injected into DVMRP.

Responding to mrinfo Requests

The Cisco IOS software answers mrinfo requests sent by mrouted systems and Cisco routers. The software returns information about neighbors on DVMRP tunnels and all of the interfaces of the router. This information includes the metric (which is always set to 1), the configured TTL threshold, the status of the interface, and various flags. The **mrinfo** EXEC command can also be used to query the router itself, as in the following example:

```
mm1-7kd# mrinfo

  171.69.214.27 (mm1-7kd.cisco.com) [version cisco 11.1] [flags: PMS]:
  171.69.214.27 -> 171.69.214.26 (mm1-r7kb.cisco.com) [1/0/pim/querier]
  171.69.214.27 -> 171.69.214.25 (mm1-45a.cisco.com) [1/0/pim/querier]
  171.69.214.33 -> 171.69.214.34 (mm1-45c.cisco.com) [1/0/pim]
  171.69.214.137 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
```

```
171.69.214.203 -> 0.0.0.0 [1/0/pim/querier/down/leaf]
171.69.214.18 -> 171.69.214.20 (mm1-45e.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.19 (mm1-45c.cisco.com) [1/0/pim]
171.69.214.18 -> 171.69.214.17 (mm1-45a.cisco.com) [1/0/pim]
```

See the “DVMRP Interoperability Example” section later in this chapter for an example of how to configure a PIM router to interoperate with a DVMRP router.

Configuring a DVMRP Tunnel

The Cisco IOS software supports DVMRP tunnels to the MBONE. You can configure a DVMRP tunnel on a router if the other end is running DVMRP. The software then sends and receives multicast packets over the tunnel. This strategy allows a PIM domain to connect to the DVMRP router in the case where all routers on the path do not support multicast routing. You cannot configure a DVMRP tunnel between two routers.

When a Cisco router runs DVMRP over a tunnel, it advertises sources in DVMRP report messages much as it does on real networks. In addition, the software caches DVMRP report messages it receives and uses them in its Reverse Path Forwarding (RPF) calculation. This behavior allows the software to forward multicast packets received over the tunnel.

When you configure a DVMRP tunnel, you should assign a tunnel an address in the following two cases:

- To enable the sending of IP packets over the tunnel
- To indicate whether the Cisco IOS software should perform DVMRP summarization

You can assign an IP address either by using the **ip address** interface configuration command, or by using the **ip unnumbered** interface configuration command to configure the tunnel to be unnumbered. Either of these two methods allows IP multicast packets to flow over the tunnel. The software will not advertise subnets over the tunnel if the tunnel has a different network number from the subnet. In this case, the software advertises only the network number over the tunnel.

To configure a DVMRP tunnel, use the following commands in interface configuration mode:

	Command	Purpose
Step 1	`Router(config-if)# `**`interface tunnel`**` `*`number`*	Specifies a tunnel interface in global configuration mode and puts the router into interface configuration mode.
Step 2	`Router(config-if)# `**`tunnel source`**` `*`ip-address`*	Sets the source address of the tunnel interface. This address is the IP address of the interface on the router.
Step 3	`Router(config-if)# `**`tunnel destination`**` `*`ip-address`*	Sets the destination adddress of the tunnel interface. This address is the IP address of the mrouted multitask router.
Step 4	`Router(config-if)# `**`tunnel mode dvmrp`**	Configures a DVMRP tunnel.

Step 5	`Router(config-if)# `**`ip address`**` `*`address mask`*
	or
	`Router(config-if)# `**`ip unnumbered`**` `*`type number`*
		Assigns an IP address to the interface.
		or
		Configures the interface as unnumbered.

Step 6	`Router(config-if)# `**`ip pim`**` [`**`dense-mode`**`	`**`sparse-mode`**`]`	Configures PIM on the interface.
Step 7	`Router(config-if)# `**`ip dvmrp accept-filter`**` `*`access-list`*` [`*`distance`*`	`**`ip neighbor-list`**` `*`access-list`*`]`	Configures an acceptance filter for incoming DVMRP reports.

See the "DVMRP Tunnel Example" section later in this chapter for an example of how to configure a DVMRP tunnel.

Advertising Network 0.0.0.0 to DVMRP Neighbors

The mrouted protocol is a public domain implementation of DVMRP. If your router is a neighbor to an mrouted Version 3.6 device, you can configure the Cisco IOS software to advertise network 0.0.0.0 to the DVMRP neighbor. Do not advertise the DVMRP default into the MBONE. You must specify whether only route 0.0.0.0 is advertised or if other routes can also be specified.

To advertise network 0.0.0.0 to DVMRP neighbors on an interface, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ip dvmrp default-information {originate | only}`	Advertises network 0.0.0.0 to DVMRP neighbors.

Advanced DVMRP Interoperability Configuration Task List

Cisco routers run PIM and know enough about DVMRP to successfully forward multicast packets to receivers and receive multicast packets from senders. It is also possible to propagate DVMRP routes into and through a PIM cloud. PIM uses this information; however, Cisco routers do not implement DVMRP to forward multicast packets.

The basic DVMRP interoperability features are described in the section "Basic DVMRP Interoperability Configuration Task List" earlier in this chapter. To configure more advanced DVMRP interoperability features on a Cisco router, perform the optional tasks described in the following sections:

- Enabling DVMRP Unicast Routing (Optional)
- Limiting the Number of DVMRP Routes Advertised (Optional)
- Changing the DVMRP Route Threshold (Optional)
- Configuring a DVMRP Summary Address (Optional)
- Disabling DVMRP Automatic summarization (Optional)
- Adding a Metric Offset to the DVMRP Route (Optional)
- Rejecting a DVMRP Nonpruning Neighbor (Optional)
- Configuring a Delay Between DVRMP Reports (Optional)

Enabling DVMRP Unicast Routing

Because policy for multicast routing and unicast routing requires separate topologies, PIM must follow the multicast topology to build loopless distribution trees. Using DVMRP unicast routing, Cisco routers and mrouted machines exchange DVMRP unicast routes, to which PIM can then reverse path forward.

Cisco routers do not perform DVMRP multicast routing among each other, but they can exchange DVMRP routes. The DVMRP routes provide a multicast topology that may differ from the unicast topology. These routes allow PIM to run over the multicast topology, thereby allowing PIM sparse mode over the MBONE topology.

When DVMRP unicast routing is enabled, the router caches routes learned in DVMRP report messages in a DVMRP routing table. PIM prefers DVMRP routes to unicast routes by default, but that preference can be configured.

DVMRP unicast routing can run on all interfaces, including generic routing encapsulation (GRE) tunnels. On DVMRP tunnels, it runs by virtue of DVMRP multicast routing. This feature does not enable DVMRP multicast routing among Cisco routers. However, if there is a DVMRP-capable multicast router, the Cisco router will do PIM/DVMRP multicast routing interaction.

To enable DVMRP unicast routing, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ip dvmrp unicast-routing`	Enables DVMRP unicast routing.

Limiting the Number of DVMRP Routes Advertised

By default, only 7000 DVMRP routes will be advertised over an interface enabled to run DVMRP (that is, a DVMRP tunnel, an interface where a DVMRP neighbor has been discovered, or an interface configured to run the **ip dvmrp unicast-routing** interface configuration command).

To change this limit, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip dvmrp route-limit count`	Changes the number of DVMRP routes advertised over an interface enabled to run DVMRP.

Changing the DVMRP Route Threshold

By default, 10,000 DVMRP routes may be received per interface within a 1-minute interval. When that rate is exceeded, a syslog message is issued, warning that a route surge might be occurring. The warning is typically used to quickly detect when routers have been misconfigured to inject a large number of routes into the MBONE.

To change the threshold number of routes that trigger the warning, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip dvmrp routehog-notification route-count`	Configures the number of routes that trigger a syslog message.

Use the **show ip igmp interface** EXEC command to display a running count of routes. When the count is exceeded, "*** ALERT ***" is appended to the line.

Configuring a DVMRP Summary Address

You can customize the summarization of DVMRP routes if the default classful automatic summarization does not suit your needs. To summarize such routes, specify a summary address by using the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **ip dvmrp summary-address** *summary-address mask* [**metric** *value*]	Specifies a DVMRP summary address.

Note At least one, more-specific route must be present in the unicast routing table before a configured summary address will be advertised.

Disabling DVMRP Automatic summarization

By default, the Cisco IOS software performs some level of DVMRP summarization automatically. Disable this function if you want to advertise all routes, not just a summary. If you configure the **ip dvmrp summary-address** interface configuration command and did not configure the **no ip dvmrp auto-summary** command, you get both custom and automatic summaries.

To disable DVMRP automatic summarization, use the following command in interface configuratioı mode:

Command	Purpose
Router(config-if)# **no ip dvmrp auto-summary**	Disables DVMRP automatic summarization.

Adding a Metric Offset to the DVMRP Route

By default, the router increments by 1 the metric of a DVMRP route advertised in incoming DVMRP reports. You can change the metric if you want to favor or not favor a certain route. The DVMRP metric is a hop count. Therefore, a very slow serial line of one hop is preferred over a route that is two hops over FDDI or another fast medium.

For example, perhaps a route is learned by Router A and the same route is learned by Router B with a higher metric. If you want to use the path through Router B because it is a faster path, you can apply a metric offset to the route learned by Router A to make it larger than the metric learned by Router B, allowing you to choose the path through Router B.

To change the default metric, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# **ip dvmrp metric-offset** [**in** | **out**] *increment*	Changes the metric added to DVMRP routes advertised in incoming reports.

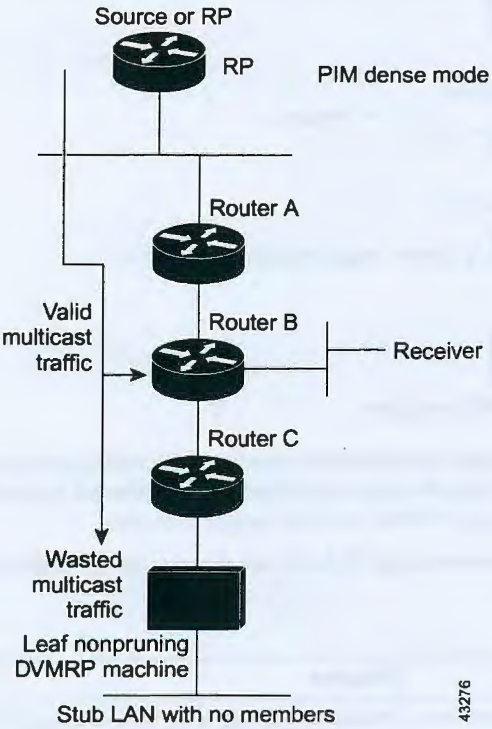
Similar to the **metric** keyword in mrouted configuration files, the following is true when using the **ip dvmrp metric-offset** interface configuration command:

- When you specify the **in** keywordor no keyword, the *increment* value is added to incoming DVMRP reports and is reported in mrinfo replies. The default value for the **in** keyword is 1.
- When you specify the **out** keyword, the *increment* is added to outgoing DVMRP reports for routes from the DVMRP routing table. The default value for the **out** keyword is 0.

Rejecting a DVMRP Nonpruning Neighbor

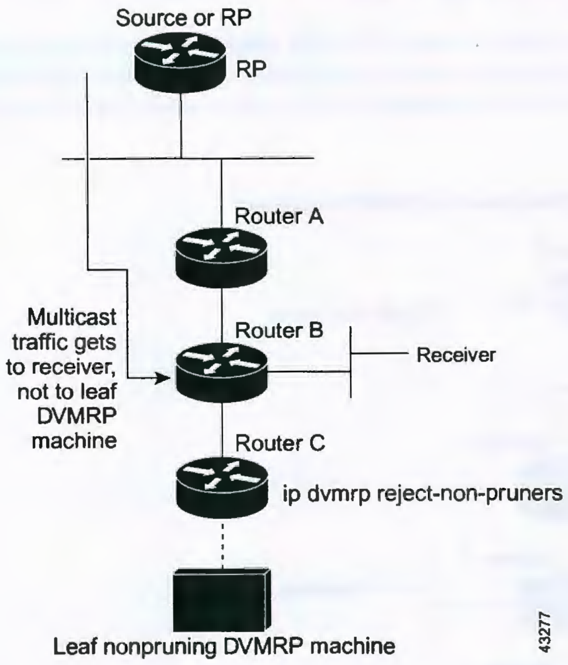
By default, Cisco routers accept all DVMRP neighbors as peers, regardless of their DVMRP capability or lack of. However, some non-Cisco machines run old versions of DVMRP that cannot prune, so they will continuously receive forwarded packets unnecessarily, wasting bandwidth. Figure 91 shows this scenario.

Figure 91 Leaf Nonpruning DVMRP Neighbor



You can prevent a router from peering (communicating) with a DVMRP neighbor if that neighbor does not support DVMRP pruning or grafting. To do so, configure Router C (which is a neighbor to the leaf, nonpruning DVMRP machine) with the **ip dvmrp reject-non-pruners** interface configuration command on the interface to the nonpruning machine. Figure 92 illustrates this scenario. In this case, when the router receives a DVMRP probe or report message without the Prune-Capable flag set, the router logs a syslog message and discards the message.

Figure 92 Router Rejects Nonpruning DVMRP Neighbor


Source or RP
RP
Router A
Multicast traffic gets to receiver, not to leaf DVMRP machine
Router B
Receiver
Router C
ip dvmrp reject-non-pruners
Leaf nonpruning DVMRP machine
43277

Note that the **ip dvmrp reject-non-pruners** command prevents peering with neighbors only. If there are any nonpruning routers multiple hops away (downstream toward potential receivers) that are not rejected, then a nonpruning DVMRP network might still exist.

To prevent peering with nonpruning DVMRP neighbors, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ip dvmrp reject-non-pruners`	Prevents peering with nonpruning DVMRP neighbors.

Configuring a Delay Between DVRMP Reports

You can configure an interpacket delay of a DVMRP report. The delay is the number of milliseconds th elapse between transmissions of sets of packets that constitute a report. The number of packets in the . is determined by the *burst* value, which defaults to 2 packets. The *milliseconds* value defaults to 100 milliseconds.

To change the default values of the delay, use the following command in interface configuration mode:

Command	Purpose

`Router(config-if)# ip dvmrp output-report-delay`
`milliseconds [burst]`
	Configures an interpacket delay between DVMRP reports.

Monitoring and Maintaining DVMRP

To clear routes from the DVMRP routing table, use the following command in EXEC mode:

Command	Purpose
`Router# clear ip dvmrp route { * | route}`	Deletes routes from the DVMRP routing table.

To display entries in the DVMRP routing table, use the following command in EXEC mode:

Command	Purpose
`Router# show ip dvmrp route [name | ip-address | type number]`	Displays the entries in the DVMRP routing table.

DVMRP Configuration Examples

This section provides the following DVMRP configuration examples:

- DVMRP Interoperability Example
- DVMRP Tunnel Example

DVMRP Interoperability Example

The following example configures DVMRP interoperability for configurations when the PIM router and the DVMRP router are on the same network segment. In this example, access list 1 advertises the networks (198.92.35.0, 198.92.36.0, 198.92.37.0, 131.108.0.0, and 150.136.0.0) to the DVMRP router, and access list 2 is used to prevent all other networks from being advertised (the **ip dvmrp metric 0** interface configuration command).

```
interface ethernet 0
 ip address 131.119.244.244 255.255.255.0
 ip pim dense-mode
 ip dvmrp metric 1 list 1
 ip dvmrp metric 0 list 2

access-list 1 permit 198.92.35.0 0.0.0.255
access-list 1 permit 198.92.36.0 0.0.0.255
access-list 1 permit 198.92.37.0 0.0.0.255
access-list 1 permit 131.108.0.0 0.0.255.255
access-list 1 permit 150.136.0.0 0.0.255.255
access-list 1 deny   0.0.0.0 255.255.255.255
access-list 2 permit 0.0.0.0 255.255.255.255
```

DVMRP Tunnel Example

The following example configures a DVMRP tunnel:

```
!
ip multicast-routing
!
interface tunnel 0
```

```
 ip unnumbered ethernet 0
 ip pim dense-mode
 tunnel source ethernet 0
 tunnel destination 192.70.92.133
 tunnel mode dvmrp
!
interface ethernet 0
 description Universitat DMZ-ethernet
 ip address 192.76.243.2 255.255.255.0
 ip pim dense-mode
```

AP 6M

Troubleshooting and Fault Management

This chapter describes basic tasks that you can perform to troubleshoot your system and the network. For detailed troubleshooting procedures and scenarios, refer to the *Internetwork Troubleshooting Guide*. For complete details on all **debug** commands, refer to the *Cisco IOS Debug Command Reference*.

For a complete description of the troubleshooting commands in this chapter, refer to the "Troubleshooting and Fault Management Commands" chapter in "Cisco IOS System Management Commands" part of the Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*. To locate documentation of other commands that appear in this chapter, use the *Cisco IOS Command Reference Master Index* or search online.

For additional troubleshooting tips, refer to the *Troubleshooting Tools* Tech Tip document on Cisco.com.

To identify hardware or software image support for a specific feature, use Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Platform Support for Cisco IOS Software Features" section in the "About Cisco IOS Software Documentation" chapter.

Troubleshooting and Fault Management Task List

To manage network faults, you need to discover, isolate, and correct problems. You can discover problems with the system monitoring commands, isolate problems with the system test commands, and resolve problems with other commands, including **debug** commands.

To perform general fault management, perform the tasks described in the following sections:

- Displaying System Information Using show Commands
- Testing Network Connectivity
- Testing Memory and Interfaces
- Logging System Error Messages
- Using Field Diagnostics on Line Cards
- Troubleshooting Specific Line Cards
- Storing Line Card Crash Information
- Creating Core Dumps
- Enabling Debug Operations
- Enabling Conditionally Triggered Debugging
- Using the Environmental Monitor

In addition to the material presented in this chapter, many chapters in the Cisco IOS software configuration guides include fault management tasks specific to certain technologies and features. You can find these tasks in the "Monitoring and Maintaining" sections.

Displaying System Information Using show Commands

To provide information about system processes, the Cisco IOS software includes an extensive list of EXEC commands that begin with the word **show**, which, when executed, display detailed tables of system information. Following is a partial list of system management **show** commands. To display the information described, use the following commands in EXEC mode, as needed:

Command	Purpose
Router# **show c2600**	Displays information about the Cisco 2600 platform, including interrupts, IOS Priority Masks, and IDMA status, for troubleshooting.
Router# **show c7200**	Displays information about the CPU and midplane for the Cisco 7200 series routers.
Router# **show context**	Displays information stored in NVRAM when the router crashes. This command is only useful to your technical support representative. This command is supported on the Cisco 2600 and 7000 series routers.
Router# **show controllers**	Displays information specific to the hardware on a line card.
Router# **show controllers logging**	Displays logging information about a line card.
Router# **show controllers tech-support**	Displays general information about a line for use when reporting a problem.
Router# **show controllers vip** *slot-number* **tech-support**	Displays information about the Versatile Interface Processor (VIP) card for use when reporting a problem
Router# **show diag**	Displays hardware information (including DRAM and static RAM details) for line cards.
Router# **show environment** [**all** | **last** | **table**]	Displays a message indicating whether an environmental warning condition currently exists, the temperature and voltage information, the last measured value from each of the six test points stored in nonvolatile memory, or environmental specifications. Examples of systems that support this comman include the Cisco 7000 and the Cisco 12000 series routers.
Router# **show gsr**	Displays hardware information on the Cisco 12000 series Gigabit Switch Router (GSR).
Router# **show gt64010**	Displays all GT64010 internal registers and interrupt status on the Cisco 7200 series routers.
Router# **show memory** [*memory-type*] [**free**] [**summary**]	Displays memory pool statistics including summary information about the activities of the system memory allocator and a block-by-block listing of memory use.
Router# **show pci** {**hardware** | **bridge** [*register*]}	Displays information about the peripheral component interconnect (PCI) hardware registers or bridge registers for the Cisco 2600 and 7000 series routers.

Command	Purpose
Router# **show processes** [**cpu**]	Displays information about all active processes.
Router# **show processes memory**	Displays information about memory usage.
Router# **show protocols**	Displays the configured protocols.
Router# **show stacks**	Displays stack usage of processes and interrupt routines, including the reason for the last system reboot. This command is only useful to your technical support representative.
Router# **show subsys** [**class** *class* | **name** *name*]	Displays subsystem information.
Router# **show tcp** [*line-number*]	Displays the status of TCP connections.
Router# **show tcp brief** [**all**]	Displays a concise description of TCP connection endpoints.
Router# **show tdm connections** [**motherboard** | **slot** *number*]	Displays a snapshot of the time-division multiplexing (TDM) bus connection or data memory in a Cisco AS5200 access server.
Router# **show tech-support** [**page**] [**password**]	Displays information about the system for use when reporting a problem.

Refer to specific **show** commands in the tables of configuration commands found throughout the chapters in Cisco IOS software configuration guides. Refer to the Cisco IOS software command reference publications for detailed descriptions of the commands.

Testing Network Connectivity

To test basic network connectivity, perform the tasks described in the following sections:

- Configuring the TCP Keepalive Packet Service
- Testing Connections with the ping Command
- Tracing Packet Routes

Configuring the TCP Keepalive Packet Service

The TCP keepalive capability allows a router to detect when the host with which it is communicating experiences a system failure, even if data stops being sent (in either direction). This capability is most useful on incoming connections. For example, if a host failure occurs while the router is communicating with a printer, the router might never notice, because the printer does not generate any traffic in the opposite direction. If keepalives are enabled, they are sent once every minute on otherwise idle connections. If 5 minutes pass and no keepalives are detected, the connection is closed. The connection is also closed if the host replies to a keepalive packet with a reset packet. This will happen if the host crashes and comes back up again.

To generate the TCP keepalive packet service, use the following command in global configuration mode:

Command	Purposes
`Router(config)# service {tcp-keepalives-in | tcp-keepalives-out}`	Generates TCP keepalive packets on idle network connections, either incoming connections initiated by a remote host, or outgoing connections initiated by a user.

Testing Connections with the ping Command

As an aid to diagnosing basic network connectivity, many network protocols support an echo protocol. The protocol involves sending a special datagram to the destination host, then waiting for a reply datagram from that host. Results from this echo protocol can help in evaluating the path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

To invoke the echo protocol, use the following command in either user or privileged EXEC mode:

Command	Purposes
`Router# ping [protocol] {host | address}`	Invokes a diagnostic tool for testing connectivity.

Refer to specific **ping** commands in the tables of configuration commands found throughout the chapters in Cisco IOS software configuration guides. Refer to the Cisco IOS software command reference publications for detailed descriptions of the command.

Tracing Packet Routes

To trace the routes that packets will actually take when traveling to their destinations, use the following command in either user or privileged EXEC mode:

Command	Purposes
`Router# trace [protocol] [destination]`	Traces packet routes through the network (privileged level).

Testing Memory and Interfaces

To test the status memory and interfaces, perform the tasks described in the following sections:

- Testing Flash Memory Status
- Testing System Memory
- Testing Interfaces Statuss

⚠ **Caution** We do not recommend using these **test** commands; they are intended to aid manufacturing personnel in checking system functionality.

Testing Flash Memory Status

To test the status of Flash memory, use the following command in privileged EXEC mode:

Command	Purposes
`Router# test flash`	Tests Flash memory on MCI and envm Flash EPROM interfaces.

Testing System Memory

To diagnose the status of system memory, use the following command in privileged EXEC mode:

Command	Purposes
`Router# test memory`	Diagnoses Multibus memory, including NVRAM.

Testing Interfaces Status

Caution Do not use this test to diagnose problems with an operational server.

To test the status of the interfaces, use the following command on a nonoperational server in privileged EXEC mode:

Command	Purposes
`Router# test interfaces`	Tests network interfaces.

Logging System Error Messages

By default, routers send **debug** EXEC command output and system error messages to a logging process. The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console. When the logging process is on, the messages are displayed on the console after the process that generated them has finished.

Note The syslog format is compatible with 4.3 Berkeley Standard Distribution (BSD) UNIX.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so error and debug output will be interspersed with prompts or output from the command.

You can set the severity level of the messages to control the type of messages displayed for the console and each destination. You can time-stamp log messages or set the syslog source address to enhance real-time debugging and management.

Refer to the *Cisco IOS Software System Error Messages* publication for detailed information on error messages.

Enabling Message Logging

Message logging is enabled by default. It must be enabled in order to send messages to any destination other than the console.

To disable message logging, use the **no logging on** command. Note that disabling the logging process can slow down the router because a process cannot continue until the messages are written to the console.

To reenable message logging after it has been disabled, use the following command in global configuration mode:

Command	Purposes
Router(config)# **logging on**	Enables message logging.

Enabling Message Logging for a Slave Card

To enable slave VIP cards to log status messages to the console (print the messages to the screen), use the following command in global configuration mode:

Command	Purposes
Router(config)# **service slave-log**	Enables slave message logging.

Setting the Error Message Display Device

If message logging is enabled, you can send messages to specified locations, in addition to the console.

To set the locations that receive messages, use the following commands in global configuration mode, as needed:

Command	Purposes
Router(config)# **logging buffered** [*size*]	Logs messages to an internal buffer.
Router(config)# **terminal monitor**	Logs messages to a nonconsole terminal.
Router(config)# **logging** *host*	Logs messages to a UNIX syslog server host.

The **logging buffered** command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging** EXEC command. The first message displayed is the oldest message in the buffer. To clear the current contents of the buffer, use the **clear logging** privileged EXEC command.

The **terminal monitor** EXEC command locally accomplishes the task of displaying the system error messages to a nonconsole terminal.

The **logging** command identifies a syslog server host to receive logging messages. The *host* argument is the name or Internet address of the host. By issuing this command more than once, you build a list of syslog servers that receive logging messages. The **no logging** command deletes the syslog server with the specified address from the list of syslogs.

Configuring Synchronization of Logging Messages

You can configure the system to synchronize unsolicited messages and **debug** command output with solicited device output and prompts for a specific line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also determine the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.

When synchronous logging of unsolicited messages and **debug** command output is turned on, unsolicited device output is displayed on the console or printed after solicited device output is displayed or printed. Unsolicited messages and **debug** command output is displayed on the console after the prompt for user input is returned. Therefore, unsolicited messages and **debug** command output are not interspersed with solicited device output and prompts. After the unsolicited messages are displayed, the console displays the user prompt again.

To configure for synchronous logging of unsolicited messages and **debug** command output with solicited device output and prompts, use the following commands beginning in global configuration mode:

	Command	Purposes
Step 1	`Router(config)# line [aux	console	vty] beginning-line-number [ending-line-number]`	Specifies the line to be configured for synchronous logging of messages.
Step 2	`Router(config-line)# logging synchronous [level severity-level	all] [limit number-of-buffers]`	Enables synchronous logging of messages.

Enabling Time-Stamps on Log Messages

By default, log messages are not time-stamped. To enable time-stamping of log messages, use either of the following commands in global configuration mode:

Command	Purposes

`Router(config)# service timestamps log uptime`
or
`Router(config)# service timestamps log datetime [msec] [localtime] [show-timezone]`
	Enables log time stamps.

Limiting the Error Message Severity Level and Facilities

You can limit the number of messages displayed to the selected device by specifying the severity level of the error message (see Table 16 for level descriptions). To do so, use the following commands in global configuration mode, as needed:

Command	Purposes
Router(config)# **logging console** *level*	Limits the number of messages logged to the console.
Router(config)# **logging monitor** *level*	Limits the number of messages logged to the terminal lines.
Router(config)# **logging trap** *level*	Limits the number of messages logged to the syslog servers.

If you have enabled syslog messages traps to be sent to a Simple Network Management Protocol (SNMP) network management station with the **snmp-server enable trap** command, you can change the level of messages sent and stored in a history table on the router. You can also change the number of messages that get stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level warning and above (see Table 16) is stored in the history table even if syslog traps are not enabled.

To change level and table size defaults, use the following commands in global configuration mode:

	Command	Purposes
Step 1	Router(config)# **logging history** *level*	Changes the default level of syslog messages stored in the history file and sent to the SNMP server.
Step 2	Router(config)# **logging history size** *number*	Changes the number of syslog messages that can be stored in the history table.

Note Table 16 lists the level keywords and severity level. For SNMP usage, the severity level values use +1. For example, **emergency** equals 1 not 0 and **critical** equals 3 not 2.

The **logging console** command limits the logging messages displayed on the console terminal to messages with a level number at or below the specified severity level, which is specified by the *level* argument. Table 16 lists the error message *level* keywords and corresponding UNIX syslog definitions in order from the most severe level to the least severe level.

Table 16 Error Message Logging Keywords

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The **no logging console** command disables logging to the console terminal.

The default is to log messages to the console at the **debugging** level and those level numbers that are lower, which means all levels. The **logging monitor** command defaults to **debugging** also. The **logging trap** command defaults to the **informational** level.

To display logging messages on a terminal, use the **terminal monitor** EXEC command.

Current software generates the following four categories of error messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**
- Output from the **debug** commands, displayed at the **debugging** level
- Interface up/down transitions and system restart messages, displayed at the **notifications** level
- Reload requests and low-process stack messages, displayed at the **informational** level

Defining the UNIX System Logging Facility

You can log messages produced by UNIX system utilities. To do this, enable this type logging and define the UNIX system facility from which you want to log messages. Table 17 lists the UNIX system facilities supported by the Cisco IOS software. Consult the operator manual for your UNIX operating system for more information about these UNIX system facilities.

To define UNIX system facility message logging, use the following command in global configuration mode:

Command	Purposes
`Router(config)# logging facility facility-type`	Configures system log facilities.

Table 17 Logging Facility Type Keywords

Facility Type Keyword	Description
auth	Indicates the authorization system.
cron	Indicates the cron facility.
daemon	Indicates the system daemon.
kern	Indicates the Kernel.
local0–7	Reserved for locally defined messages.
lpr	Indicates line printer system.
mail	Indicates mail system.
news	Indicates USENET news.
sys9	Indicates system use.
sys10	Indicates system use.
sys11	Indicates system use.
sys12	Indicates system use.
sys13	Indicates system use.
sys14	Indicates system use.
syslog	Indicates the system log.

Table 17 Logging Facility Type Keywords (continued)

Facility Type Keyword	Description
user	Indicates user process.
uucp	Indicates UNIX-to-UNIX copy system.

Displaying Logging Information

To display logging information, use the following commands in EXEC mode, as needed:

Command	Purposes
`Router# show logging`	Displays the state of syslog error and event logging, including host addresses, whether console logging is enabled, and other logging statistics.
`Router# show controllers vip slot-number logging`	Displays the state of syslog error and event logging of a VIP card, including host addresses, whether console logging i enabled, and other logging statistics
`Router# show logging history`	Displays information in the syslog history table such as the table size, the status of messages, and the text of the messages stored in the table.

Logging Errors to a UNIX Syslog Daemon

To configure the syslog daemon on a 4.3 BSD UNIX system, include a line such as the following in the /etc/syslog.conf file:

```
local7.debugging /usr/adm/logs/cisco.log
```

The **debugging** keyword specifies the syslog level; see Table 16 for a general description of other keywords. The **local7** keyword specifies the logging facility to be used; see Table 17 for a general description of other keywords.

The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

Setting the Syslog Source Address

By default, a syslog message contains the IP address of the interface it uses to leave the router. To set all syslog messages to contain the same IP address, regardless of which interface they use, use the following command in global configuration mode:

Command	Purposes
`Router(config)# logging source-interface type number`	Sets the syslog source address.

Using Field Diagnostics on Line Cards

Each line card on the Cisco 12000 series routers can perform field diagnostic testing to isolate faulty hardware without disrupting normal operation of the system. However, performing field diagnostic testing on a line card does halt all activity on the line card for the duration of the testing. After successful completion of the field diagnostic testing, the Cisco IOS software is automatically reloaded on the line card.

Note The field diagnostic **diag** command must be executed from the Gigabit Route Processor (GRP) main console port.

To perform field diagnostic testing on a line card, use the following command in privileged EXEC mode:

Command	Purposes
`Router# diag slot-number [previous | post | verbose | wait]`	Specifies the line card on which you want to perform diagnostic testing. Optionally, specifies that previous test results are displayed, that only extended power-on self-tests (POST) be performed, that the maximum messages are displayed, or that the Cisco IOS software not be reloaded on the line card after successful completion of the tests. The following prompt is displayed: `Running Diags will halt ALL activity on the requested slot. [confirm]` At the prompt, press **Return** to confirm that you want to perform field diagnostic testing on the specified line card, or type **no** to stop the testing.

To stop field diagnostic testing on a line card, use either of the following commands in privileged EXEC mode:

Command	Purpose

`Router# diag slot-number halt`
or
`Router# no diag slot-number`
	Specifies the line card on which you want to stop diagnostic testing.

Note When you stop the field diagnostic test, the line card remains down (that is, in an unbooted state). In most cases, you stopped the testing because you need to remove the line card or replace the line card. If that is not the case and you want to bring the line card back up (that is, online), you must use the **microcode reload** global configuration command or power cycle the line card.

Troubleshooting Specific Line Cards

Cisco IOS provides the **execute-on** command to allow you to issue Cisco IOS commands (such as **show** commands) to a specific line card for monitoring and maintenance. For example, you could show which Cisco IOS image is loaded on the card in slot 3 of a Cisco 12012 Gigabit Switch Router (GSR) by issuing the **execute-on slot 3 show version** command. You can also use this command for troubleshooting cards in the dial shelf of Cisco access servers. For complete documentation of this command, refer to the "Troubleshooting" chapter of the Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*.

Storing Line Card Crash Information

This section explains how to enable storing of crash information for a line card and optionally specify the type and amount of information stored. Technical support representatives need to be able to look at the crash information from the line card to troubleshoot serious problems on the line card. The crash information contains all the line card memory information, including the main memory and transmit and receive buffer information.

⚠ **Caution** Use the **exception linecard** global configuration command only when directed by a technical support representative, and only enable options that the technical support representative requests you to enable.

To enable and configure the crash information options for a line card, use the following command in global configuration mode:

Command	Purpose
Router(config)# **exception linecard** {**all** | **slot** *slot-number*} [**corefile** *filename* | **main-memory** *size* [**k** | **m**] | **queue-ram** *size* [**k** | **m**] | **rx-buffer** *size* [**k** | **m**] | **sqe-register-rx** | **sqe-register-tx** | **tx-buffer** *size* [**k** | **m**]]	Specifies the line card for which you want crash information when a line card resets. Optionally, specify the type and amount of memory to be stored.

Creating Core Dumps

When your router crashes, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the crash. Not all crash types will produce a core dump.

Core dumps are generally useful only to your technical support representative. The core dump file, which is a very large binary file, must be transferred to a Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), or remote copy protocol (rcp) server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

⚠ **Caution** Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation.

To configure your system to generate core dump files, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **ip ftp password** [*encrypt-type*] *password*	(Optional for core dump file transfers using FTP) Specifies the password to be used for FTP connections.
Router(config)# **ip ftp username** *username*	(Optional for core dump file transfers using FTP) Configures the user name for FTP connections.
Router(config)# **exception protocol** {**ftp** | **rcp** | **tftp**}	Configures the protocol used for core dumps.
Router(config)# **exception flash**	Configures the router for a core dump using a Flash disk.
Router(config)# **exception core-file** *name*	Specifies the name of the core dump file when your router has generated a core dump file after crashing.
Router(config)# **exception dump** *ip-address*	Configures the router to dump a core file to a particular server when the router crashes.
Router(config)# **exception memory** {**fragment** *size* | **minimum** *size*}	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
Router(config)# **exception spurious-interrupt** [*number*]	Causes the router to create a core dump and reboot after a specified number of spurious interrupts.

Specifying the Protocol for the Core Dump

To configure the router to generate a core dum, perform the tasks described in the following sections:

- Using TFTP for Core Dumps
- Using FTP for Core Dumps
- Using rcp for Core Dumps
- Using a Flash Disk

Using TFTP for Core Dumps

Due to a limitation of most TFTP applications, the router will dump only the first 16 MB of the core file. Therefore, if your router's main memory is larger than 16 MB, do not use TFTP.

To configure a router for a core dump using TFTP, use the following commands in global configuration mode:

Command	Purpose
Router(config)# **exception protocol tftp**	Specifies that the TFTP protocol should be used for core dumps.
Router(config)# **exception dump** *ip-address*	Configures the router to dump a core file to a particular server when the router crashes.

For example, the following command configures a router for a core dump using TFTP, where 172.17.92.2 is the IP address of the TFTP server:

```
Router(config)# exception protocol tftp
Router(config)# exception dump 172.17.92.2
```

The core dump is written to a file named *hostname*-core on the TFTP server, where *hostname* is the name of the router (in the example, the file would be named Router-core). You can change the name of the core file by adding the **exception core-file** *filename* configuration command.

Depending on the TFTP server application used, it may be necessary to create, on the TFTP server, the empty target file to which the router can write the core. Also, make sure that there is enough memory on your TFTP server to hold the complete core dump.

Using FTP for Core Dumps

To configure the router for a core dump using FTP, use the following commands in global configuration mode:

	Command	Purposes
Step 1	`Router(config)# ip ftp username username`	(Optional) Configures the user name for FTP connections.
Step 2	`Router(config)# ip ftp password [type] password`	(Optional) Specifies the password to be used for FTP connections.
Step 3	`Router(config)# exception protocol ftp`	Specifies that FTP should be used for core dump file transfers.
Step 4	`Router(config)# exception dump ip-address`	Configures the router to dump a core file to a particular server when the router crashes.
Step 5	`Router(config)# exception core-file name`	Specifies the name of the core dump file when your router has generated a core dump file after crashing.

The following example configures a router to use FTP to dump a core file named dumpfile to the FTP server at 172.17.92.2 when it crashes.

```
ip ftp username red
ip ftp password blue
exception protocol ftp
exception dump 172.17.92.2
exception core-file dumpfile
```

Using rcp for Core Dumps

You can use rcp to capture a core dump. Enabling rcp on a router is described in the “Configuring a Router to Use rcp” section of the “Configuring Basic File Transfer Services” chapter.

To enable rcp on the router, use the following commands in global configuration mode to capture the core dump:

	Command	Purposes
Step 1	`Router(config)# exception protocol ftp`	Specifies that rcp should be used for core dump file transfers.
Step 2	`Router(config)# exception dump ip-address`	Configures the router to dump a core file to a particular server when the router crashes.

The following example sets 172.17.92.2 as the IP address of the host on which rcp is enabled:

```
exception protocol rcp
exception dump 172.17.92.2
```

Using a Flash Disk for Core Dumps

Some router platforms support the Flash disk as an alternative to the linear Flash memory or Personal Computer Memory Card Industry Association (PCMCIA) Flash card. The large storage capacity of these Flash disks makes them good candidates for another means of capturing a core dump. To configure a router for a core dump using a Flash disk, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **`exception flash`** `[`**`procmem`** `|`**`iomem`** `|` **`all`**`]` *`device-name`*`[:`*`partition-number`*`] [`**`erase`** `|` **`no_erase`**`]`	Configures the router for a core dump using a flash disk.

The **show flash all** EXEC command will list the devices you can use for the **exception flash** command.

Specifying the Name of the Core Dump File

To specify a filename of a core dump file when the router crashes, use the following command in global configuration mode:

Command	Purpose
`Router(config)#` **`exception core-file`** *`name`*	Specifies the name of the core dump file when your router has generated a core dump file after crashing.

Creating an Exception Memory Core Dump

To cause the router to create a core dump and reboot when certain memory size parameters are violated during the debugging process, use the following commands in global configuration mode:

Command	Purpose
`Router(config)#` **`exception memory fragment`** *`size`*	The minimum contiguous block of memory in the free pool (in bytes).
`Router(config)#` **`exception memory minimum`** *`size`*	The minimum size of the free memory pool (in bytes).

The size parameter is expressed in bytes and is checked every 60 seconds. If you enter a size that is greater than the free memory and the **exception dump** command has been configured, a core dump and router reload is generated after 60 seconds. If the **exception dump** command is not configured, the router reloads without triggering a core dump. The following example configures the router to monitor the free memory. If the memory falls below 250,000 bytes, the core dump is created and the router reloads.

```
exception dump 172.16.92.2
exception core-file memory.overrun
exception memory minimum 250000
```

Setting a Spurious Interrupt Core Dump

During the debugging process, you can configure the router to create a spurious interrupt core dump and reboot when a specified number of interrupts have occurred.

Caution Use the exception spurious-interrupt global configuration command only when directed by a technical support representative and only enable options requested by the technical support representative.

To enable and configure the crash information for spurious interrupts, use the following command in global configuration mode:

Command	Purpose
`Router(config)# exception spurious-interrupt number`	Sets the maximum number of spurious interrupts to include in the core dump before reloading.

The following example configures a router to create a core dump with a limit of two spurious interrupts:

```
exception spurious-interrupt 2
```

Enabling Debug Operations

Your router includes hardware and software to aid in troubleshooting internal problems and problems with other hosts on the network. The **debug** privileged EXEC mode commands start the console display of several classes of network events. The following commands describe in general the system debug message feature. Refer to the *Cisco IOS Debug Command Reference* for all information regarding **debug** commands. Also refer to the *Internetwork Troubleshooting Guide* publication for additional information.

To enable debugging operations, use the following commands:

Command	Purposes
`Router# show debugging`	Displays the state of each debugging option.
`Router# debug ?`	Displays a list and brief description of all the **debug** command options.
`Router# debug command`	Begins message logging for the specified **debug** command.
`Router# no debug command`	Turns message logging off for the specified **debug** command.

Caution The system gives high priority to debugging output. For this reason, debugging commands should be turned on only for troubleshooting specific problems or during troubleshooting sessions with technical support personnel. Excessive debugging output can render the system inoperable.

You can configure time-stamping of system **debug** messages. Time-stamping enhances real-time debugging by providing the relative timing of logged events. This information is especially useful when customers send debugging output to your technical support personnel for assistance. To enable time-stamping of system **debug** messages, use either of the following commands in global configuration mode:

Command	Purposes

`Router(config)# service timestamps debug uptime`
or
`Router(config)# service timestamps debug datetime [msec] [localtime] [show-timezone]`
	Enables time-stamping of system **debug** messages.

Normally, the messages are displayed only on the console terminal. Refer to the section "Setting the Error Message Display Device" earlier in this chapter to change the output device.

Enabling Conditionally Triggered Debugging

When the Conditionally Triggered Debugging feature is enabled, the router generates debugging messages for packets entering or leaving the router on a specified interface; the router will not generate debugging output for packets entering or leaving through a different interface. You can specify the interfaces explicitly. For example, you may only want to see debugging messages for one interface or subinterface. You can also turn on debugging for all interfaces that meet specified condition. This feature is useful on dial access servers, which have a large number of ports.

Normally, the router will generate debugging messages for every interface, resulting in a large number of messages. The large number of messages consumes system resources, and can affect your ability to find the specific information you need. By limiting the number of debugging messages, you can receive messages related to only the ports you wish to troubleshoot.

Conditionally Triggered Debugging controls the output from the following protocol-specific **debug** commands:

- **debug aaa** {**accounting** | **authorization** | **authentication**}
- **debug dialer** {**events** | **packets**}
- **debug isdn** {**q921** | **q931**}
- **debug modem** {**oob** | **trace**}
- **debug ppp** {**all** | **authentication** | **chap** | **error** | **negotiation** | **multilink events** | **packet**}

Although this feature limits the output of the commands listed, it does not automatically enable the generation of debugging output from these commands. Debugging messages are generated only when the protocol-specific **debug** command is enabled. The **debug** command output is controlled through two processes:

- The protocol-specific **debug** commands specify which protocols are being debugged. For example, the **debug dialer events** command generates debugging output related to dialer events.
- The **debug condition** commands limit these debugging messages to those related to a particular interface. For example, the **debug condition username bob** command generates debugging output only for interfaces with packets that specify a username of bob.

To configure Conditionally Triggered Debugging, perform the tasks described in the following sections:

- Enabling Protocol-Specific debug Commands
- Enabling Conditional Debugging Commands
- Specifying Multiple Debugging Conditions

Enabling Protocol-Specific debug Commands

In order to generate any debugging output, the protocol-specific **debug** command for the desired output must be enabled. Use the **show debugging** command to determine which types of debugging are enabled. To display the current debug conditions, use the **show debug condition** command. To enable the desired protocol-specific **debug** commands, use the following commands in privileged EXEC mode :

Command	Purpose
`Router#` **`show debugging`**	Determines which types of debugging are enabled.
`Router#` **`show debug condition`** `[`*`condition-id`*`]`	Displays the current **debug** conditions.
`Router#` **`debug`** *`protocol`*	Enables the desired debugging commands.
`Router#` **`no debug`** *`protocol`*	Disables the debugging commands that are not desired.

If you do not want output, disable all the protocol-specific **debug** commands.

Enabling Conditional Debugging Commands

If no **debug condition** commands are enabled, all debugging output, regardless of the interface, will be displayed for the enabled protocol-specific **debug** commands.

The first **debug condition** command you enter enables conditional debugging. The router will display only messages for interfaces that meet one of the specified conditions. If multiple conditions are specified, the interface must meet at least one of the conditions in order for messages to be displayed.

To enable messages for interfaces specified explicitly or for interfaces that meet certain conditions, perform the tasks described in the following sections:

- Displaying Messages for One Interface
- Displaying Messages for Multiple Interfaces
- Limiting the Number of Messages Based on Conditions

Displaying Messages for One Interface

To disable debugging messages for all interfaces except one, use the following command in privileged EXEC mode:

Command	Purpose
`Router#` **`debug condition interface`** *`interface`*	Enables debugging output for only the specified interface.

To reenable debugging output for all interfaces, use the **no debug interface** command.

Displaying Messages for Multiple Interfaces

To enable debugging messages for multiple interfaces, use the following commands in privileged EXEC mode:

	Command	Purposes
Step 1	`Router# debug condition interface interface`	Enables debugging output for only the specified interface
Step 2	`Router# debug condition interface interface`	Enable debugging messages for additional interfaces. Repeat this task until debugging messages are enabled for all desired interfaces.

If you specify more than one interface by entering this command multiple times, debugging output will be displayed for all of the specified interfaces. To turn off debugging on a particular interface, use the **no debug interface** command. If you use the **no debug interface all** command or remove the last **debug interface** command, debugging output will be reenabled for all interfaces.

Limiting the Number of Messages Based on Conditions

The router can monitor interfaces to learn if any packets contain the specified value for one of the following conditions:

- username
- calling party number
- called party number

If you enter a condition, such as calling number, debug output will be stopped for all interfaces. The router will then monitor every interface to learn if a packet with the specified calling party number is sent or received on any interfaces. If the condition is met on an interface or subinterface, **debug** command output will be displayed for that interface. The debugging output for an interface is "triggered" when the condition has been met. The debugging output continues to be disabled for the other interfaces. If, at some later time, the condition is met for another interface, the debug output also will become enabled for that interface.

Once debugging output has been triggered on an interface, the output will continue until the interface goes down. However, the session for that interface might change, resulting in a new username, called party number, or calling party number. Use the **no debug interface** command to reset the debug trigger mechanism for a particular interface. The debugging output for that interface will be disabled until the interface meets one of the specified conditions.

To limit the number of debugging messages based on a specified condition, use the following command in privileged EXEC mode:

Command	Purpose
`Router# debug condition {username username	called dial-string	caller dial-string}`	Enables conditional debugging. The router will display only messages for interfaces that meet this condition.

To reenable the debugging output for all interfaces, enter the **no debug condition all** command.

Specifying Multiple Debugging Conditions

To limit the number of debugging messages based on more than one condition, use the following commands in privileged EXEC mode:

	Command	Purposes
Step 1	`Router# debug condition {username username | called dial-string | caller dial-string}`	Enables conditional debugging, and specifies the first condition.
Step 2	`Router# debug condition {username username | called dial-string | caller dial-string}`	Specifies the second condition. Repeat this task until all conditions are specified.

If you enter multiple **debug condition** commands, debugging output will be generated if an interface meets at least one of the conditions. If you remove one of the conditions using the **no debug condition** command, interfaces that meet only that condition no longer will produce debugging output. However, interfaces that meet a condition other than the removed condition will continue to generate output. Only if no active conditions are met for an interface will the output for that interface be disabled.

Conditionally Triggered Debugging Configuration Examples

In this example, four conditions have been set by the following commands:

- **debug condition interface serial 0**
- **debug condition interface serial 1**
- **debug condition interface virtual-template 1**
- **debug condition username fred**

The first three conditions have been met by one interface. The fourth condition has not yet been met:

```
Router# show debug condition

Condition 1: interface Se0 (1 flags triggered)
        Flags: Se0
Condition 2: interface Se1 (1 flags triggered)
        Flags: Se1
Condition 3: interface Vt1 (1 flags triggered)
        Flags: Vt1
Condition 4: username fred (0 flags triggered)
```

When any **debug condition** command is entered, debugging messages for conditional debugging are enabled. The following debugging messages show conditions being met on different interfaces as the serial 0 and serial 1 interfaces come up. For example, the second line of output indicates that serial interface 0 meets the username fred condition.

```
*Mar  1 00:04:41.647: %LINK-3-UPDOWN: Interface Serial0, changed state to up
*Mar  1 00:04:41.715: Se0 Debug: Condition 4, username fred triggered, count 2
*Mar  1 00:04:42.963: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed
state to up
*Mar  1 00:04:43.271: Vi1 Debug: Condition 3, interface Vt1 triggered, count 1
*Mar  1 00:04:43.271: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
*Mar  1 00:04:43.279: Vi1 Debug: Condition 4, username fred triggered, count 2
*Mar  1 00:04:43.283: Vi1 Debug: Condition 1, interface Se0 triggered, count 3
*Mar  1 00:04:44.039: %IP-4-DUPADDR: Duplicate address 172.27.32.114 on Ethernet 0,
sourced by 00e0.1e3e.2d41
```

```
*Mar  1 00:04:44.283: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to up
*Mar  1 00:04:54.667: %LINK-3-UPDOWN: Interface Serial1, changed state to up
*Mar  1 00:04:54.731: Se1 Debug: Condition 4, username fred triggered, count 2
*Mar  1 00:04:54.735: Vi1 Debug: Condition 2, interface Se1 triggered, count 4
*Mar  1 00:04:55.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed
state to up
```

After a period of time, the **show debug condition** command displays the revised list of conditions:

```
Router# show debug condition

Condition 1: interface Se0 (2 flags triggered)
        Flags: Se0 Vi1
Condition 2: interface Se1 (2 flags triggered)
        Flags: Se1 Vi1
Condition 3: interface Vt1 (2 flags triggered)
        Flags: Vt1 Vi1
Condition 4: username fred (3 flags triggered)
        Flags: Se0 Vi1 Se1
```

Next, the serial 1 and serial 0 interfaces go down. When an interface goes down, conditions for that interface are cleared.

```
*Mar  1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed state to down
*Mar  1 00:05:51.471: Se1 Debug: Condition 4, username fred cleared, count 1
*Mar  1 00:05:51.479: Vi1 Debug: Condition 2, interface Se1 cleared, count 3
*Mar  1 00:05:52.443: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed
state to down
*Mar  1 00:05:56.859: %LINK-3-UPDOWN: Interface Serial0, changed state to down
*Mar  1 00:05:56.887: Se0 Debug: Condition 4, username fred cleared, count 1
*Mar  1 00:05:56.895: Vi1 Debug: Condition 1, interface Se0 cleared, count 2
*Mar  1 00:05:56.899: Vi1 Debug: Condition 3, interface Vt1 cleared, count 1
*Mar  1 00:05:56.899: Vi1 Debug: Condition 4, username fred cleared, count 0
*Mar  1 00:05:56.903: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down
*Mar  1 00:05:57.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed
state to down
*Mar  1 00:05:57.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
changed state to down
```

The final **show debug condition** output is the same as the output before the interfaces came up:

```
Router# show debug condition

Condition 1: interface Se0 (1 flags triggered)
        Flags: Se0
Condition 2: interface Se1 (1 flags triggered)
        Flags: Se1
Condition 3: interface Vt1 (1 flags triggered)
        Flags: Vt1
Condition 4: username fred (0 flags triggered)
```

Using the Environmental Monitor

Some routers and access servers have an environmental monitor that monitors the physical condition of the router. If a measurement exceeds acceptable margins, a warning message is printed to the system console. The system software collects measurements once every 60 seconds, but warnings for a given test point are printed at most once every 4 hours. If the temperature measurements are out of specification more than the shutdown, the software shuts the router down (the fan will remain on). The router must be manually turned off and on after such a shutdown. You can query the environmental monitor using the **show environment** command at any time to determine whether a measurement is out of tolerance. Refer to the *Cisco IOS System Error Messages* publication for a description of environmental monitor warning messages.

On routers with an environmental monitor, if the software detects that any of its temperature test points have exceeded maximum margins, it performs the following steps:

1. Saves the last measured values from each of the six test points to internal nonvolatile memory.
2. Interrupts the system software and causes a shutdown message to be printed on the system console.
3. Shuts off the power supplies after a few milliseconds of delay.

The system displays the following message if temperatures exceed maximum margins, along with a message indicating the reason for the shutdown:

```
Router#
%ENVM-1-SHUTDOWN: Environmental Monitor initiated shutdown
%ENVM-2-TEMP: Inlet temperature has reached SHUTDOWN level at 64(C)
```

Refer to the hardware installation and maintenance publication for your router for more information about environmental specifications.

AP GN

Configuring IP Routing Protocol-Independent Features

This chapter describes how to configure IP routing protocol-independent features. For a complete description of the IP routing protocol-independent commands in this chapter, refer to the "IP Routing Protocol-Independent Commands" chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication. To locate documentation of other commands in this chapter, use the command reference master index, or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter in this book.

Protocol-Independent Feature Task List

Previous chapters addressed configurations of specific routing protocols. To configure optional protocol-independent features, perform any of the tasks described in the following sections:

- Using Variable-Length Subnet Masks (Optional)
- Configuring Static Routes (Optional)
- Specifying Default Routes (Optional)
- Changing the Maximum Number of Paths (Optional)
- Configuring Multi-Interface Load Splitting (Optional)
- Redistributing Routing Information (Optional)
- Filtering Routing Information (Optional)
- Enabling Policy Routing (Optional)
- Managing Authentication Keys (Optional)
- Monitoring and Maintaining the IP Network (Optional)

See the section "IP Routing Protocol-Independent Configuration Examples" at the end of this chapter for configuration examples.

7425
6

Using Variable-Length Subnet Masks

Enhanced IGRP (EIGRP), Intermediate System-to-Intermediate System (IS-IS) Interdomain Routing Protocol, Open Shortest Path First (OSPF), Routing Information Protocol (RIP) Version 2, and static routes support variable-length subnet masks (VLSMs). With VLSMs, you can use different masks for the same network number on different interfaces, which allows you to conserve IP addresses and more efficiently use available address space. However, using VLSMs also presents address assignment challenges for the network administrator and ongoing administrative challenges.

Refer to RFC 1219 for detailed information about VLSMs and how to correctly assign addresses.

Note Consider your decision to use VLSMs carefully. You can easily make mistakes in address assignments and you will generally find it more difficult to monitor your network using VLSMs.

Note The best way to implement VLSMs is to keep your existing numbering plan in place and gradually migrate some networks to VLSMs to recover address space. See the "Variable-Length Subnet Mask Example" section at the end of this chapter for an example of using VLSMs.

Configuring Static Routes

Static routes are user-defined routes that cause packets moving between a source and a destination to take a specified path. Static routes can be important if the Cisco IOS software cannot build a route to a particular destination. They are useful for specifying a gateway of last resort to which all unroutable packets will be sent.

To configure a static route, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip route prefix mask {ip-address | interface-type interface-number} [distance] [tag tag] [permanent]`	Establishes a static route.

See the "Overriding Static Routes with Dynamic Protocols Example" section at the end of this chapter for an example of configuring static routes.

The software remembers static routes until you remove them (using the **no** form of the **ip route** global configuration command). However, you can override static routes with dynamic routing information through prudent assignment of administrative distance values. Each dynamic routing protocol has a default administrative distance, as listed in Table 9. If you would like a static route to be overridden by information from a dynamic routing protocol, simply ensure that the administrative distance of the static route is higher than that of the dynamic protocol.

Table 9 Dynamic Routing Protocol Default Administrative Distances

Route Source	Default Distance
Connected interface	0
Static route	1

Table 9 Dynamic Routing Protocol Default Administrative Distances (continued)

Route Source	Default Distance
Enhanced IGRP (EIGRP) summary route	5
Exterior Border Gateway Protocol (BGP)	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Interior BGP	200
Unknown	255

Static routes that point to an interface will be advertised via RIP, IGRP, and other dynamic routing protocols, regardless of whether **redistribute static** router configuration commands were specified for those routing protocols. These static routes are advertised because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. However, if you define a static route to an interface that is not one of the networks defined in a **network** command, no dynamic routing protocols will advertise the route unless a **redistribute static** command is specified for these protocols.

When an interface goes down, all static routes through that interface are removed from the IP routing table. Also, when the software can no longer find a valid next hop for the address specified as the address of the forwarding router in a static route, the static route is removed from the IP routing table.

Specifying Default Routes

A router might not be able to determine the routes to all other networks. To provide complete routing capability, the common practice is to use some routers as *smart routers* and give the remaining routers default routes to the smart router. (Smart routers have routing table information for the entire internetwork.) These default routes can be passed along dynamically, or can be configured into the individual routers.

Most dynamic interior routing protocols include a mechanism for causing a smart router to generate dynamic default information that is then passed along to other routers.

Specifying a Default Network

If a router has a directly connected interface onto the specified default network, the dynamic routing protocols running on that device will generate or source a default route. In the case of RIP, the router will advertise the pseudonetwork 0.0.0.0. In the case of IGRP, the network itself is advertised and flagged as an exterior route.

A router that is generating the default for a network also may need a default of its own. One way a router can generate its own default is to specify a static route to the network 0.0.0.0 through the appropriate device.

To define a static route to a network as the static default route, use the following command in global configuration mode:

Command	Purpose
Router(config)# **ip default-network** *network-number*	Specifies a default network.

Understanding Gateway of Last Resort

When default information is being passed along through a dynamic routing protocol, no further configuration is required. The system periodically scans its routing table to choose the optimal default network as its default route. In the case of RIP, there is only one choice, network 0.0.0.0. In the case of IGRP, there might be several networks that can be candidates for the system default. The Cisco IOS software uses both administrative distance and metric information to determine the default route (gateway of last resort). The selected default route appears in the gateway of last resort display of the **show ip route** EXEC command.

If dynamic default information is not being passed to the software, candidates for the default route are specified with the **ip default-network** global configuration command. In this usage, the **ip default-network** command takes an unconnected network as an argument. If this network appears in the routing table from any source (dynamic or static), it is flagged as a candidate default route and is a possible choice as the default route.

If the router has no interface on the default network, but does have a route to it, it considers this network as a candidate default path. The route candidates are examined and the best one is chosen, based on administrative distance and metric. The gateway to the best default path becomes the gateway of last resort.

Changing the Maximum Number of Paths

By default, most IP routing protocols install a maximum of four parallel routes in a routing table. Static routes always install six routes. The exception is BGP, which by default allows only one path to a destination.

The range of maximum paths is one to six paths. To change the maximum number of parallel paths allowed, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# **maximum-paths** *maximum*	Configures the maximum number of parallel paths allowed in a routing table.

Configuring Multi-Interface Load Splitting

Multi-interface load splitting allows you to efficiently control traffic that travels across multiple interfaces to the same destination. The **traffic-share min** router configuration command specifies that if multiple paths are available to the same destination, only paths with the minimum metric will be installed in the routing table. The number of paths allowed is never more than six. For dynamic routing protocols, the number of paths is controlled by the **maximum-paths** router configuration command. The static route source can always install six paths. If more paths are available, the extra paths are discarded. If some installed paths are removed from the routing table, pending routes are added automatically.

When the **traffic-share min** command is used with the **across-interfaces** keyword, an attempt is made to use as many different interfaces as possible to forward traffic to the same destination. When the maximum path limit has been reached and a new path is installed, the router compares the installed paths. For example, if path X references the same interface as path Y and the new path uses a different interface, path X is removed and the new path is installed.

To configure traffic that is distributed among multiple routes of unequal cost for equal cost paths across multiple interfaces, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# traffic-share min {across-interfaces}`	Configures multi-interface load splitting across different interfaces with equal cost paths.

Redistributing Routing Information

In addition to running multiple routing protocols simultaneously, the Cisco IOS software can redistribute information from one routing protocol to another. For example, you can instruct the software to readvertise IGRP-derived routes using RIP, or to readvertise static routes using the IGRP protocol. Redistributing information from one routing protocol to another applies to all of the IP-based routing protocols.

You also can conditionally control the redistribution of routes between routing domains by defining a method known as *route maps* between the two domains.

The following four tables list tasks associated with route redistribution. Although redistribution is a protocol-independent feature, some of the **match** and **set** commands are specific to a particular protocol.

To define a route map for redistribution, use the following command in global configuration mode:

Command	Purpose
`Router(config)# route-map map-tag [permit	deny] [sequence-number]`	Defines any route maps needed to control redistribution.

One or more **match** commands and one or more **set** commands typically follow a **route-map** global configuration command. If there are no **match** commands, then everything matches. If there are no **set** commands, nothing is done (other than the match). Therefore, you need at least one **match** or **set** command.

To define conditions for redistributing routes from one routing protocol into another, use at least one of the following commands in route-map configuration mode, as needed:

Command	Purpose
`Router(config-route-map)# match as-path path-list-number`	Matches a BGP autonomous system path access list.
`Router(config-route-map)# match community-list community-list-number [exact]`	Matches a BGP community list.

Command	Purpose
Router(config-route-map)# **match ip address** {*access-list-number* | *access-list-name*} [*...access-list-number* | *...access-list-name*]	Matches a standard access list.
Router(config-route-map)# **match metric** *metric-value*	Matches the specified metric.
Router(config-route-map)# **match ip next-hop** {*access-list-number* | *access-list-name*} [*access-list-number* | *access-list-name*]	Matches a next-hop router address passed by one of the access lists specified.
Router(config-route-map)# **match tag** *tag-value* [*tag-value*]	Matches the specified tag value.
Router(config-route-map)# **match interface** *interface-type interface-number* [*interface-type interface-number*]	Matches the specified next hop route out one of the interfaces specified.
Router(config-route-map)# **match ip route-source** {*access-list-number* | *access-list-name*} [*access-list-number* | *access-list-name*]	Matches the address specified by the specified advertised access lists.
Router(config-route-map)# **match route-type** {**local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2**}	Matches the specified route type.

One or more **match** commands and one or more **set** commands should follow a **route-map** router configuration command. To define conditions for redistributing routes from one routing protocol into another, use at least one of the following commands in route-map configuration mode as needed:

Command	Purpose
Router(config-route-map)# **set community** {*community-number* [**additive**]} | **none**	Sets the communities attribute.
Router(config-route-map)# **set dampening** *halflife reuse suppress max-suppress-time*	Sets BGP route dampening factors.
Router(config-route-map)# **set local-preference** *number-value*	Assigns a value to a local BGP path.
Router(config-route-map)# **set weight** *weight*	Specifies the BGP weight for the routing table.
Router(config-route-map)# **set origin** {**igp** | **egp** *as-number* | **incomplete**}	Sets the BGP origin code.
Router(config-route-map)# **set as-path** {**tag** | **prepend** *as-path-string*}	Modifies the BGP autonomous system path.
Router(config-route-map)# **set next-hop** *next-hop*	Specifies the address of the next hop.
Router(config-route-map)# **set automatic-tag**	Enables automatic computing of the tag table.
Router(config-route-map)# **set level** {**level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone**}	Specifies the areas in which to import routes.
Router(config-route-map)# **set metric** *metric-value*	Sets the metric value to give the redistributed routes (for any protocol except IGRP or Enhanced IGRP [EIGRP]).
Router(config-route-map)# **set metric** *bandwidth delay reliability loading mtu*	Sets the metric value to give the redistributed routes (for IGRP or EIGRP only).
Router(config-route-map)# **set metric-type** {**internal** | **external** | **type-1** | **type-2**}	Sets the metric type to give redistributed routes.

Command	Purpose
Router(config-route-map)# **set metric-type internal**	Sets the Multi Exit Discriminator (MED) value on prefixes advertised to Exterior BGP neighbor to match the Interior Gateway Protocol (IGP) metric of the next hop.
Router(config-route-map)# **set tag** *tag-value*	Sets the tag value to associate with the redistributed routes.

See the "BGP Route Map Examples" section in the "Configuring BGP" chapter for examples of BGP route maps. See the "BGP Community with Route Maps Examples" section in the "Configuring BGP" chapter for examples of BGP communities and route maps.

To distribute routes from one routing domain into another and to control route redistribution, use the following commands in router configuration mode:

	Command	Purpose
Step 1	Router(config-router)# **redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [**metric** *metric-value*] [**metric-type** *type-value*] [**match internal** | **external** *type-value*] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]	Redistributes routes from one routing protocol to another routing protocol.
Step 2	Router(config-router)# **default-metric** *number*	Causes the current routing protocol to use the same metric value for all redistributed routes (BGP, OSPF, RIP).
Step 3	Router(config-router)# **default-metric** *bandwidth delay reliability loading mtu*	Causes the IGRP or Enhanced IGRP (EIGRP) routing protocol to use the same metric value for all non-IGRP redistributed routes.
Step 4	Router(config-router)# **no default-information** {**in** | **out**}	Disables the redistribution of default information between IGRP processes, which is enabled by default.

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count and the IGRP metric is a combination of five quantities. In such situations, an artificial metric is assigned to the redistributed route. Because of this unavoidable tampering with dynamic information, carelessly exchanging routing information between different routing protocols can create routing loops, which can seriously degrade network operation.

Understanding Supported Metric Translations

This section describes supported automatic metric translations between the routing protocols. The following descriptions assume that you have not defined a default redistribution metric that replaces metric conversions:

- RIP can automatically redistribute static routes. It assigns static routes a metric of 1 (directly connected).
- BGP does not normally send metrics in its routing updates.

- IGRP can automatically redistribute static routes and information from other IGRP-routed autonomous systems. IGRP assigns static routes a metric that identifies them as directly connected. IGRP does not change the metrics of routes derived from IGRP updates from other autonomous systems.
- Note that any protocol can redistribute other routing protocols if a default metric is in effect.

Filtering Routing Information

To filter routing protocol information performing the tasks in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional:

- Preventing Routing Updates Through an Interface (Required)
- Controlling the Advertising of Routes in Routing Updates (Optional)
- Controlling the Processing of Routing Updates (Optional)
- Filtering Sources of Routing Information (Optional)

Note When routes are redistributed between OSPF processes, no OSPF metrics are preserved.

Preventing Routing Updates Through an Interface

To prevent other routers on a local network from learning about routes dynamically, you can keep routing update messages from being sent through a router interface. Keeping routing update messages from being sent through a router interface prevents other systems on the interface from learning about routes dynamically. This feature applies to all IP-based routing protocols except BGP.

OSPF and IS-IS behave somewhat differently. In OSPF, the interface address you specify as passive appears as a stub network in the OSPF domain. OSPF routing information is neither sent nor received through the specified router interface. In IS-IS, the specified IP addresses are advertised without actually running IS-IS on those interfaces.

To prevent routing updates through a specified interface, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)# passive-interface interface-type interface-number`	Suppresses the sending of routing updates through the specified interface.

See the "Passive Interface Examples" section at the end of this chapter for examples of configuring passive interfaces.

Configuring Default Passive Interfaces

In Internet service provider (ISP) and large enterprise networks, many of the distribution routers have more than 200 interfaces. Before the introduction of the Default Passive Interface feature, there were two possibilities for obtaining routing information from these interfaces:

- Configure a routing protocol such as OSPF on the backbone interfaces and redistribute connected interfaces.
- Configure the routing protocol on all interfaces and manually set most of them as passive.

Network managers may not always be able to summarize type 5 link-state advertisements (LSAs) at the router level where redistribution occurs, as in the first possibility. Thus, a large number of type 5 LSAs can be flooded over the domain.

In the second possibility, large type 1 LSAs might be flooded into the area. The Area Border Router (ABR) creates type 3 LSAs, one for each type 1 LSA, and floods them to the backbone. It is possible, however, to have unique summarization at the ABR level, which will inject only one summary route into the backbone, thereby reducing processing overhead.

The prior solution to this problem was to configure the routing protocol on all interfaces and manually set the **passive-interface** router configuration command on the interfaces where adjacency was not desired. But in some networks, this solution meant coding 200 or more passive interface statements. With the Default Passive Interface feature, this problem is solved by allowing all interfaces to be set as passive by default using a single **passive-interface default** command, then configuring individual interfaces where adjacencies are desired using the **no passive-interface** command.

Thus, the Default Passive Interface feature simplifies the configuration of distribution routers and allows the network manager to obtain routing information from the interfaces in large ISP and enterprise networks.

To set all interfaces as passive by default and then activate only those interfaces that need to have adjacencies set, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **`router`** *`protocol`*	Configures the routing protocol on the network.
Step 2	`Router(config-router)#` **`passive-interface default`**	Sets all interfaces as passive by default.
Step 3	`Router(config-router)#` **`no passive-interface`** *`interface-type`*	Activates only those interfaces that need to have adjacencies set.
Step 4	`Router(config-router)#` **`network`** *`network-address`* `[`*`options`*`]`	Specifies the list of networks for the routing process. The *network-address* argument is an IP address written in dotted decimal notation—172.24.101.14, for example.

See the section "Default Passive Interface Example" at the end of this chapter for an example of a default passive interface.

To verify that interfaces on your network have been set to passive, you could enter a network monitoring command such as the **show ip ospf interface** EXEC command, or you could verify the interfaces you enabled as active using a command such as the **show ip interface** EXEC command.

Controlling the Advertising of Routes in Routing Updates

To prevent other routers from learning one or more routes, you can suppress routes from being advertised in routing updates. Suppressing routes in route updates prevents other routers from learning the interpretation of a particular device of one or more routes. You cannot specify an interface name in OSPF. When used for OSPF, this feature applies only to external routes.

To suppress routes from being advertised in routing updates, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)#` **`distribute-list`** {*`access-list-number`* | *`access-list-name`*} **`out`** [*`interface-name`* | *`routing-process`* | *`as-number`*]	Permits or denies routes from being advertised in routing updates depending upon the action listed in the access list.

Controlling the Processing of Routing Updates

You might want to avoid processing certain routes listed in incoming updates. This feature does not apply to OSPF or IS-IS. To suppress routes in incoming updates, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)#` **`distribute-list`** {*`access-list-number`* | *`access-list-name`*} **`in`** [*`interface-type interface-number`*]	Suppresses routes listed in updates from being processed.

Filtering Sources of Routing Information

Filtering sources of routing information prioritizes routing information from different sources, because some pieces of routing information may be more accurate than others. An *administrative distance* is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. In a large network, some routing protocols and some routers can be more reliable than others as sources of routing information. Also, when multiple routing processes are running in the same router for IP, it is possible for the same route to be advertised by more than one routing process. By specifying administrative distance values, you enable the router to intelligently discriminate between sources of routing information. The router will always pick the route whose routing protocol has the lowest administrative distance.

To filter sources of routing information, use the following command in router configuration mode:

Command	Purpose
`Router(config-router)#` **`distance`** {*`ip-address`* {*`wildcard-mask`*}} [*`ip-standard-list`*] [*`ip-extended`*]	Filters on routing information sources.

There are no general guidelines for assigning administrative distances because each network has its own requirements. You must determine a reasonable matrix of administrative distances for the network as a whole. Table 9 shows the default administrative distance for various routing information sources.

For example, consider a router using IGRP and RIP. Suppose you trust the IGRP-derived routing information more than the RIP-derived routing information. In this example, because the default IGRP administrative distance is lower than the default RIP administrative distance, the router uses the IGRP-derived information and ignores the RIP-derived information. However, if you lose the source of the IGRP-derived information (because of a power shutdown in another building, for example), the router uses the RIP-derived information until the IGRP-derived information reappears.

For an example of filtering on sources of routing information, see the section "Administrative Distance Examples" later in this chapter.

Note You also can use administrative distance to rate the routing information from routers running the same routing protocol. This application is generally discouraged if you are unfamiliar with this particular use of administrative distance, because it can result in inconsistent routing information, including forwarding loops.

Note The weight of a route can no longer be set with the **distance** command. To set the weight for a route, use a route-map.

Enabling Policy Routing

Policy routing is a more flexible mechanism for routing packets than destination routing. It is a process whereby the router puts packets through a route map before routing them. The route map determines which packets are routed to which router next. You might enable policy routing if you want certain packets to be routed some way other than the obvious shortest path. Possible applications for policy routing are to provide equal access, protocol-sensitive routing, source-sensitive routing, routing based on interactive versus batch traffic, and routing based on dedicated links.

To enable policy routing, you must identify which route map to use for policy routing and create the route map. The route map itself specifies the match criteria and the resulting action if all of the match clauses are met. These steps are described in the following task tables.

To enable policy routing on an interface, indicate which route map the router should use by using the following command in interface configuration mode. All packets arriving on the specified interface will be subject to policy routing. This command disables fast switching of all packets arriving on this interface.

Command	Purpose
`Router(config-if)# ip policy route-map map-tag`	Identifies the route map to use for policy routing.

To define the route map to be used for policy routing, use the following command in global configuration mode:

Command	Purpose
`Router(config)# route-map map-tag [permit	deny] [sequence-number]`	Defines a route map to control where packets are output.

To define the criteria by which packets are examined to learn if they will be policy-routed, use either one or both of the following commands in route-map configuration mode. No match clause in the route map indicates all packets.

Command	Purpose
Router(config-route-map)# **match length** *minimum-length maximum-length*	Matches the Level 3 length of the packet.
Router(config-route-map)# **match ip address** {*access-list-number* | *access-list-name*} [*access-list-number* | *access-list-name*]	Matches the destination IP address that is permitted by one or more standard or extended access lists.

To set the precedence and specify where the packets that pass the match criteria are output, use the following commands in route-map configuration mode:

	Command	Purpose
Step 1	Router(config-route-map)# **set ip precedence** *number* | *name*	Sets the precedence value in the IP header.
Step 2	Router(config-route-map)# **set ip next-hop** *ip-address* [*ip-address*]	Specifies the next hop to which to route the packet. (It must be an adjacent router).
Step 3	Router(config-route-map)# **set interface** *interface-type interface-number* [... *interface-type interface-number*]	Specifies the output interface for the packet.
Step 4	Router(config-route-map)# **set ip default next-hop** *ip-address* [*ip-address*]	Specifies the next hop to which to route the packet, if there is no explicit route for this destination. **Note** Like the **set ip next-hop** command, the **set ip default next-hop** command needs to specify an adjacent router.
Step 5	Router(config-route-map)# **set default interface** *interface-type interface-number* [... *interface-type interface-number*]	Specifies the output interface for the packet, if there is no explicit route for this destination.

Note The **set ip next-hop** and **set ip default next-hop** are similar commands but have a different order of operations. Configuring the **set ip next-hop** command causes the system to use policy routing first and then use the routing table. Configuring the **set ip default next-hop** causes the system to use the routing table first and then policy route the specified next hop.

The precedence setting in the IP header determines whether, during times of high traffic, the packets will be treated with more or less precedence than other packets. By default, the Cisco IOS software leaves this value untouched; the header remains with the precedence value it had.

The precedence bits in the IP header can be set in the router when policy routing is enabled. When the packets containing those headers arrive at another router, the packets are ordered for transmission according to the precedence set, if the queueing feature is enabled. The router does not honor the precedence bits if queueing is not enabled; the packets are sent in FIFO order.

You can change the precedence setting, using either a number or name. The names came from RFC 791, but are evolving. You can enable other features that use the values in the **set ip precedence** route-map configuration command to determine precedence. Table 10 lists the possible numbers and their corresponding name, from least important to most important.

Table 10 IP Precedence Values

Number	Name
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

The **set** commands can be used with each other. They are evaluated in the order shown in the previous task table. A usable next hop implies an interface. Once the local router finds a next hop and a usable interface, it routes the packet.

To display the cache entries in the policy route cache, use the **show ip cache policy** EXEC command.

If you want policy routing to be fast switched, see the following section "Enabling Fast-Switched Policy Routing."

See the "Policy Routing Example" section at the end of this chapter for an example of policy routing.

Enabling Fast-Switched Policy Routing

IP policy routing can now be fast switched. Prior to fast-switched policy routing, policy routing could only be process switched, which meant that on most platforms, the switching rate was approximately 1000 to 10,000 packets per second. Such rates were not fast enough for many applications. Users that need policy routing to occur at faster speeds can now implement policy routing without slowing down the router.

Fast-switched policy routing supports all of the **match** commands and most of the **set** commands, except for the following restrictions:

- The **set ip default** command is not supported.
- The **set interface** command is supported only over point-to-point links, unless a route cache entry exists using the same interface specified in the **set interface** command in the route map. Also, at the process level, the routing table is consulted to determine if the interface is on a reasonable path to the destination. During fast switching, the software does not make this check. Instead, if the packet matches, the software blindly forwards the packet to the specified interface.

Policy routing must be configured before you configure fast-switched policy routing. Fast switching of policy routing is disabled by default. To have policy routing be fast switched, use the following command in interface configuration mode:

Command	Purpose
`Router(config-if)# ip route-cache policy`	Enables fast switching of policy routing.

Enabling Local Policy Routing

Packets that are generated by the router are not normally policy routed. To enable local policy routing for such packets, indicate which route map the router should use by using the following command in global configuration mode. All packets originating on the router will then be subject to local policy routing.

Command	Purpose
`Router(config)# ip local policy route-map map-tag`	Identifies the route map to use for local policy routing.

Use the **show ip local policy** EXEC command to display the route map used for local policy routing, if one exists.

Enabling NetFlow Policy Routing

NetFlow policy routing (NPR) integrates policy routing, which enables traffic engineering and traffic classification, with NetFlow services, which provide billing, capacity planning, and monitoring information on real-time traffic flows. IP policy routing now works with Cisco Express Forwarding (CEF), distributed CEF (dCEF), NetFlow, and NetFlow flow acceleration.

As quality of service (QoS) and traffic engineering become more popular, so does interest in the ability of policy routing to selectively set IP Precedence and type of service (ToS) bits (based on access lists and packet size), thereby routing packets based on predefined policy. It is important that policy routing work well in large, dynamic routing environments. Hence, distributed support allows customers to leverage their investment in distributed architecture.

NetFlow policy routing leverages the following technologies:

- CEF, which looks at a Forwarding Information Base (FIB) instead of a routing table when switching packets, to address maintenance problems of a demand caching scheme.
- dCEF, which addresses the scalability and maintenance problems of a demand caching scheme.
- NetFlow, which allows accounting, capacity planning, traffic monitoring, and flow-accelerating specific applications.

Following are NPR benefits:

- NPR takes advantage of the new switching services. CEF, dCEF, and NetFlow can now use policy routing.
- Now that policy routing is integrated into CEF, policy routing can be deployed on a wide scale and on high-speed interfaces.

Following are NPR restrictions:

- NPR is only available on Cisco IOS platforms that support CEF.
- Distributed FIB-based policy routing is only available on platforms that support dCEF.
- The Cisco 12000 platform currently is not supported.

- Policy routing will not be flow accelerated if any match packet-size clause of a route map is configured. Because packet size is not part of a flow definition, a policy routing decision cannot be based on a flow entry.
- The **set ip next-hop verify-availability** route-map configuration command of route-map is not supported in dCEF because dCEF does not support the Cisco Discovery Protocol (CDP) database.

In order for NetFlow policy routing to work, the following features must already be configured:

- CEF, dCEF, or NetFlow
- Policy routing

To configure CEF, dCEF, or NetFlow, refer to the appropriate chapter of the *Cisco IOS Switching Services Configuration Guide*.

NPR is the default policy routing mode. No additional configuration tasks are required to enable policy routing in conjunction with CEF, dCEF, or NetFlow. As soon as one of these features is turned on, packets are automatically subject to policy routing in the appropriate switching path.

There is one new, optional configuration command (**set ip next-hop verify-availability**). This command has the following restrictions:

- It can cause some performance degradation due to CDP database lookup overhead per packet.
- CDP must be enabled on the interface.
- The directly connected next hop must be a Cisco device with CDP enabled.
- It is supported in NetFlow accelerated policy routing, but not available in dCEF, due to the dependency of the CDP neighbor database.

It is assumed that policy routing itself is already configured.

If the router is policy routing packets to the next hop and the next hop happens to be down, the router will try unsuccessfully to use Address Resolution Protocol (ARP) for the next hop (which is down). This behavior will continue forever.

To prevent this situation, you can configure the router to first verify that the next hops of the route map are CDP neighbors of the router before routing to that next hop.

This task is optional because some media or encapsulations do not support CDP, or it may not be a Cisco device that is sending the router traffic.

To configure the router to verify that the next hop is a CDP neighbor before the router tries to policy route to it, use the following command in route-map configuration mode:

Command	Purpose
`Router(config-route-map)# set ip next-hop verify-availability`	Causes the router to confirm that the next hops of the route map are CDP neighbors of the router.

If the command shown is set and the next hop is not a CDP neighbor, the router looks to the subsequent next hop, if there is one. If there is none, the packets simply are not policy routed.

If the command shown is not set, the packets are either policy routed or remain forever unrouted.

If you want to selectively verify availability of only some next hops, you can configure different route-map entries (under the same route map name) with different criteria (using access list matching or packet size matching), and use the **set ip next-hop verify-availability** configuration command selectively.

Typically, you would use existing policy routing and NetFlow **show** EXCEC commands to monitor these features. For more information on these **show** commands, refer to the "IP Routing Protocol-Independent Commands" chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication for policy routing commands and the appropriate chapter of the *Cisco IOS Switching Services Command Reference* publication for NetFlow commands.

To display the route map Inter Processor Communication (IPC) message statistics in the Route Processor (RP) or Versatile Interface Processor (VIP), use the following command in EXEC mode:

Command	Purpose
Router# **show route-map ipc**	Displays the route map IPC message statistics in the RP or VIP.

Managing Authentication Keys

Key management is a method of controlling authentication keys used by routing protocols. Not all protocols can use key management. Authentication keys are available for Director Response Protocol (DRP) Agent, Enhanced IGRP (EIGRP), and RIP Version 2.

Before you manage authentication keys, authentication must be enabled. See the appropriate protocol chapter to learn how to enable authentication for that protocol.

To manage authentication keys, define a key chain, identify the keys that belong to the key chain, and specify how long each key is valid. Each key has its own key identifier (specified with the **key** key chain configuration command), which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use.

You can configure multiple keys with lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters. The lifetimes allow for overlap during key changes. Note that the router must know the time. Refer to the Network Time Protocol (NTP) and calendar commands in the "Performing Basic System Management" chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

To manage authentication keys, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)#**key chain** *name-of-chain*	Identifies a key chain.
Step 2	Router(config-keychain)# **key** *number*	Identifies the key number in key chain configuration mode.
Step 3	Router(config-keychain-key)# **key-string** *text*	Identifies the key string in key chain configuration mode.
Step 4	Router(config-keychain-key)# **accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}]	Specifies the time period during which the key can be received.
Step 5	Router(config-keychain-key)# **send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}	Specifies the time period during which the key can be sent.

Use the **show key chain** EXEC command to display key chain information. For examples of key management, see the "Key Management Examples" section at the end of this chapter.

Monitoring and Maintaining the IP Network

You can remove all contents of a particular cache, table, or database. You also can display specific statistics. The following sections describe each of these tasks.

Clearing Routes from the IP Routing Table

You can remove all contents of a particular table. Clearing a table can become necessary when the contents of the particular structure have become, or are suspected to be, invalid.

To clear one or more routes from the IP routing table, use the following command in EXEC mode:

Command	Purpose
`Router# clear ip route {network [mask] | *}`	Clears one or more routes from the IP routing table.

Displaying System and Network Statistics

You can display specific statistics such as the contents of IP routing tables, caches, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path packets leaving your device are taking through the network.

To display various routing statistics, use the following commands in EXEC mode, as needed:

Command	Purpose
`Router# show ip cache policy`	Displays the cache entries in the policy route cache.
`Router# show ip local policy`	Displays the local policy route map if one exists.
`Router# show ip policy`	Displays policy route maps.
`Router# show ip protocols`	Displays the parameters and current state of the active routing protocol process.
`Router# show ip route [address [mask] [longer-prefixes]] | [protocol [process-id]]`	Displays the current state of the routing table.
`Router# show ip route summary`	Displays the current state of the routing table in summary form.
`Router# show ip route supernets-only`	Displays supernets.
`Router# show key chain [name-of-chain]`	Displays authentication key information.
`Router# show route-map [map-name]`	Displays all route maps configured or only the one specified.

IP Routing Protocol-Independent Configuration Examples

The following sections provide routing protocol-independent configuration examples:

- Variable-Length Subnet Mask Example
- Overriding Static Routes with Dynamic Protocols Example
- Administrative Distance Examples
- Static Routing Redistribution Example
- IGRP Redistribution Example
- RIP and IGRP Redistribution Example
- EIGRP Redistribution Examples
- RIP and EIGRP Redistribution Examples
- OSPF Routing and Route Redistribution Examples
- Default Metric Values Redistribution Example
- Route Map Examples
- Passive Interface Examples
- Policy Routing Example
- NetFlow Policy Routing Example
- Key Management Examples

Variable-Length Subnet Mask Example

In the following example, a 14-bit subnet mask is used, leaving two bits of address space reserved for serial line host addresses. There is sufficient host address space for two host endpoints on a point-to-point serial link.

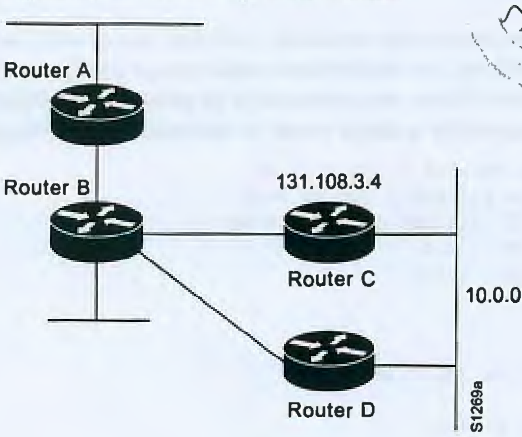
```
interface ethernet 0
 ip address 131.107.1.1 255.255.255.0
! 8 bits of host address space reserved for ethernets

interface serial 0
 ip address 131.107.254.1 255.255.255.252
! 2 bits of address space reserved for serial lines

! Router is configured for OSPF and assigned AS 107
router ospf 107
! Specifies network directly connected to the router
 network 131.107.0.0 0.0.255.255 area 0.0.0.0
```

Overriding Static Routes with Dynamic Protocols Example

In the following example, packets for network 10.0.0.0 from Router B (where the static route is installed) will be routed through 131.108.3.4 if a route with an administrative distance less than 110 is not available. Figure 60 illustrates this example. The route learned by a protocol with an administrative distance of less than 110 might cause Router B to send traffic destined for network 10.0.0.0 via the alternate path—through Router D.

```
ip route 10.0.0.0 255.0.0.0 131.108.3.4 110
```

Figure 60 Overriding Static Routes



Administrative Distance Examples

In the following example, the **router igrp** global configuration command sets up IGRP routing in autonomous system 109. The **network** router configuration commands specify IGRP routing on networks 192.31.7.0 and 128.88.0.0. The first **distance** router configuration command sets the default administrative distance to 255, which instructs the router to ignore all routing updates from routers for which an explicit distance has not been set. The second **distance** command sets the administrative distance to 90 for all routers on the Class C network 192.31.7.0. The third **distance** command sets the administrative distance to 120 for the router with the address 128.88.1.3.

```
router igrp 109
 network 192.31.7.0
 network 128.88.0.0
 distance 255
 distance 90 192.31.7.0 0.0.0.255
 distance 120 128.88.1.3 0.0.0.0
```

The following example assigns the router with the address 192.31.7.18 an administrative distance of 100, and all other routers on subnet 192.31.7.0 an administrative distance of 200:

```
distance 100 192.31.7.18 0.0.0.0
distance 200 192.31.7.0 0.0.0.255
```

However, if you reverse the order of these commands, all routers on subnet 192.31.7.0 are assigned an administrative distance of 200, including the router at address 192.31.7.18:

```
distance 200 192.31.7.0 0.0.0.255
distance 100 192.31.7.18 0.0.0.0
```

Assigning administrative distances is a problem unique to each network and is done in response to the greatest perceived threats to the connected network. Even when general guidelines exist, the network manager must ultimately determine a reasonable matrix of administrative distances for the network as a whole.

In the following example, the distance value for IP routes learned is 90. Preference is given to these IP routes rather than routes with the default administrative distance value of 110.

```
router isis
 distance 90 ip
```

Static Routing Redistribution Example

In the example that follows, three static routes are specified, two of which are to be advertised. The static routes are created by specifying the **redistribute static** router configuration command, then specifying an access list that allows only those two networks to be passed to the IGRP process. Any redistributed static routes should be sourced by a single router to minimize the likelihood of creating a routing loop.

```
ip route 192.1.2.0 255.255.255.0 192.31.7.65
ip route 193.62.5.0 255.255.255.0 192.31.7.65
ip route 131.108.0.0 255.255.255.0 192.31.7.65
access-list 3 permit 192.1.2.0
access-list 3 permit 193.62.5.0
!
router igrp 109
 network 192.31.7.0
 default-metric 10000 100 255 1 1500
 redistribute static
 distribute-list 3 out static
```

7407
3

IGRP Redistribution Example

Each IGRP routing process can provide routing information to only one autonomous system; the Cisco IOS software must run a separate IGRP process and maintain a separate routing database for each autonomous system it services. However, you can transfer routing information between these routing databases.

Suppose the router has one IGRP routing process for network 15.0.0.0 in autonomous system 71 and another for network 192.31.7.0 in autonomous system 109, as the following commands specify:

```
router igrp 71
 network 15.0.0.0
router igrp 109
 network 192.31.7.0
```

To transfer a route to 192.31.7.0 into autonomous system 71 (without passing any other information about autonomous system 109), use the command in the following example:

```
router igrp 71
 redistribute igrp 109
 distribute-list 3 out igrp 109
access-list 3 permit 192.31.7.0
```

RIP and IGRP Redistribution Example

Consider a WAN at a university that uses RIP as an interior routing protocol. Assume that the university wants to connect its WAN to a regional network, 128.1.0.0, which uses IGRP as the routing protocol. The goal in this case is to advertise the networks in the university network to the routers on the regional network. The commands for the interconnecting router are listed in the example that follows:

```
router igrp 109
 network 128.1.0.0
 redistribute rip
 default-metric 10000 100 255 1 1500
 distribute-list 10 out rip
```

In this example, the **router** global configuration command starts an IGRP routing process. The **network** router configuration command specifies that network 128.1.0.0 (the regional network) is to receive IGRP routing information. The **redistribute** router configuration command specifies that RIP-derived routing information be advertised in the routing updates. The **default-metric** router configuration command assigns an IGRP metric to all RIP-derived routes.

The **distribute-list** router configuration command instructs the Cisco IOS software to use access list 10 (not defined in this example) to limit the number of entries in each outgoing update. The access list prevents unauthorized advertising of university routes to the regional network.

EIGRP Redistribution Examples

Each Enhanced IGRP (EIGRP) routing process provides routing information to only one autonomous system. The Cisco IOS software must run a separate EIGRP process and maintain a separate routing database for each autonomous system it services. However, you can transfer routing information between these routing databases.

Suppose the software has one EIGRP routing process for network 15.0.0.0 in autonomous system 71 and another for network 192.31.7.0 in autonomous system 109, as the following commands specify:

```
router eigrp 71
 network 15.0.0.0
router eigrp 109
 network 192.31.7.0
```

To transfer a route from 192.31.7.0 into autonomous system 71 (without passing any other information about autonomous system 109), use the command in the following example:

```
router eigrp 71
 redistribute eigrp 109 route-map 109-to-71
 route-map 109-to-71 permit
 match ip address 3
 set metric 10000 100 1 255 1500
access-list 3 permit 192.31.7.0
```

The following example is an alternative way to transfer a route to 192.31.7.0 into autonomous system 71. Unlike the previous configuration, this one does not allow you to arbitrarily set the metric.

```
router eigrp 71
 redistribute eigrp 109
 distribute-list 3 out eigrp 109
access-list 3 permit 192.31.7.0
```

RIP and EIGRP Redistribution Examples

This section provides a simple RIP redistribution example and a complex redistribution example between Enhanced IGRP (EIGRP) and BGP.

Simple Redistribution Example

Consider a WAN at a university that uses RIP as an interior routing protocol. Assume that the university wants to connect its WAN to a regional network, 128.1.0.0, which uses Enhanced IGRP (EIGRP) as the routing protocol. The goal in this case is to advertise the networks in the university network to the routers on the regional network.

The commands for the interconnecting router are listed in the example that follows:

```
router eigrp 109
 network 128.1.0.0
 redistribute rip
 default-metric 10000 100 255 1 1500
 distribute-list 10 out rip
```

In this example, the **router** global configuration command starts an EIGRP routing process. The **network** router configuration command specifies that network 128.1.0.0 (the regional network) is to send and receive EIGRP routing information. The **redistribute** router configuration command specifies that RIP-derived routing information be advertised in the routing updates. The **default-metric** router configuration command assigns an EIGRP metric to all RIP-derived routes.

The **distribute-list** router configuration command instructs the Cisco IOS software to use access list 10 (not defined in this example) to limit the entries in each outgoing update. The access list prevents unauthorized advertising of university routes to the regional network.

Complex Redistribution Example

The most complex redistribution case is one in which *mutual* redistribution is required between an IGP (in this case EIGRP) and BGP.

Suppose that BGP is running on a router somewhere else in autonomous system 1, and that the BGP routes are injected into EIGRP routing process 1. You must use filters to ensure that the proper routes are advertised. The example configuration for router R1 illustrates use of access filters and a distribution list to filter routes advertised to BGP neighbors. This example also illustrates configuration commands for redistribution between BGP and EIGRP.

```
! Configuration for router R1:
router bgp 1
 network 131.108.0.0
 neighbor 192.5.10.1 remote-as 2
 neighbor 192.5.10.15 remote-as 1
 neighbor 192.5.10.24 remote-as 3
 redistribute eigrp 1
 distribute-list 1 out eigrp 1
!
! All networks that should be advertised from R1 are controlled with access lists:
!
access-list 1 permit 131.108.0.0
access-list 1 permit 150.136.0.0
access-list 1 permit 128.125.0.0
!
router eigrp 1
 network 131.108.0.0
 network 192.5.10.0
 redistribute bgp 1
```

OSPF Routing and Route Redistribution Examples

OSPF typically requires coordination among many internal routers, ABRs, and Autonomous System Boundary Routers (ASBRs). At a minimum, OSPF-based routers can be configured with all default parameter values, with no authentication, and with interfaces assigned to areas.

Three types of examples follow:

- The first examples are simple configurations illustrating basic OSPF commands.
- The second example illustrates a configuration for an internal router, ABR, and ASBRs within a single, arbitrarily assigned, OSPF autonomous system.
- The third example illustrates a more complex configuration and the application of various tools available for controlling OSPF-based routing environments.

Basic OSPF Configuration Examples

The following example illustrates a simple OSPF configuration that enables OSPF routing process 9000, attaches Ethernet interface 0 to area 0.0.0.0, and redistributes RIP into OSPF, and OSPF into RIP:

```
interface ethernet 0
 ip address 130.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1
 ip address 130.94.1.1 255.255.255.0
!
router ospf 9000
 network 130.93.0.0 0.0.255.255 area 0.0.0.0
 redistribute rip metric 1 subnets
!
router rip
 network 130.94.0.0
 redistribute ospf 9000
 default-metric 1
```

The following example illustrates the assignment of four area IDs to four IP address ranges. In the example, OSPF routing process 109 is initialized, and four OSPF areas are defined: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, while area 0 enables OSPF for *all other* networks.

```
router ospf 109
 network 131.108.20.0 0.0.0.255 area 10.9.50.0
 network 131.108.0.0 0.0.255.255 area 2
 network 131.109.10.0 0.0.0.255 area 3
 network 0.0.0.0 255.255.255.255 area 0
!
! Interface Ethernet0 is in area 10.9.50.0:
interface ethernet 0
 ip address 131.108.20.5 255.255.255.0
!
! Interface Ethernet1 is in area 2:
interface ethernet 1
 ip address 131.108.1.5 255.255.255.0
!
! Interface Ethernet2 is in area 2:
interface ethernet 2
 ip address 131.108.2.5 255.255.255.0
!
! Interface Ethernet3 is in area 3:
interface ethernet 3
 ip address 131.109.10.5 255.255.255.0
!
! Interface Ethernet4 is in area 0:
interface ethernet 4
 ip address 131.109.1.1 255.255.255.0
!
```

7403
6

```
! Interface Ethernet5 is in area 0:
interface ethernet 5
 ip address 10.1.0.1 255.255.0.0
```

Each **network** router configuration command is evaluated sequentially, so the specific order of these commands in the configuration is important. The Cisco IOS software sequentially evaluates the address/wildcard-mask pair for each interface. See the "IP Routing Protocols Commands" chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication for more information.

Consider the first **network** command. Area ID 10.9.50.0 is configured for the interface on which subnet 131.108.20.0 is located. Assume that a match is determined for interface Ethernet 0. Interface Ethernet 0 is attached to Area 10.9.50.0 only.

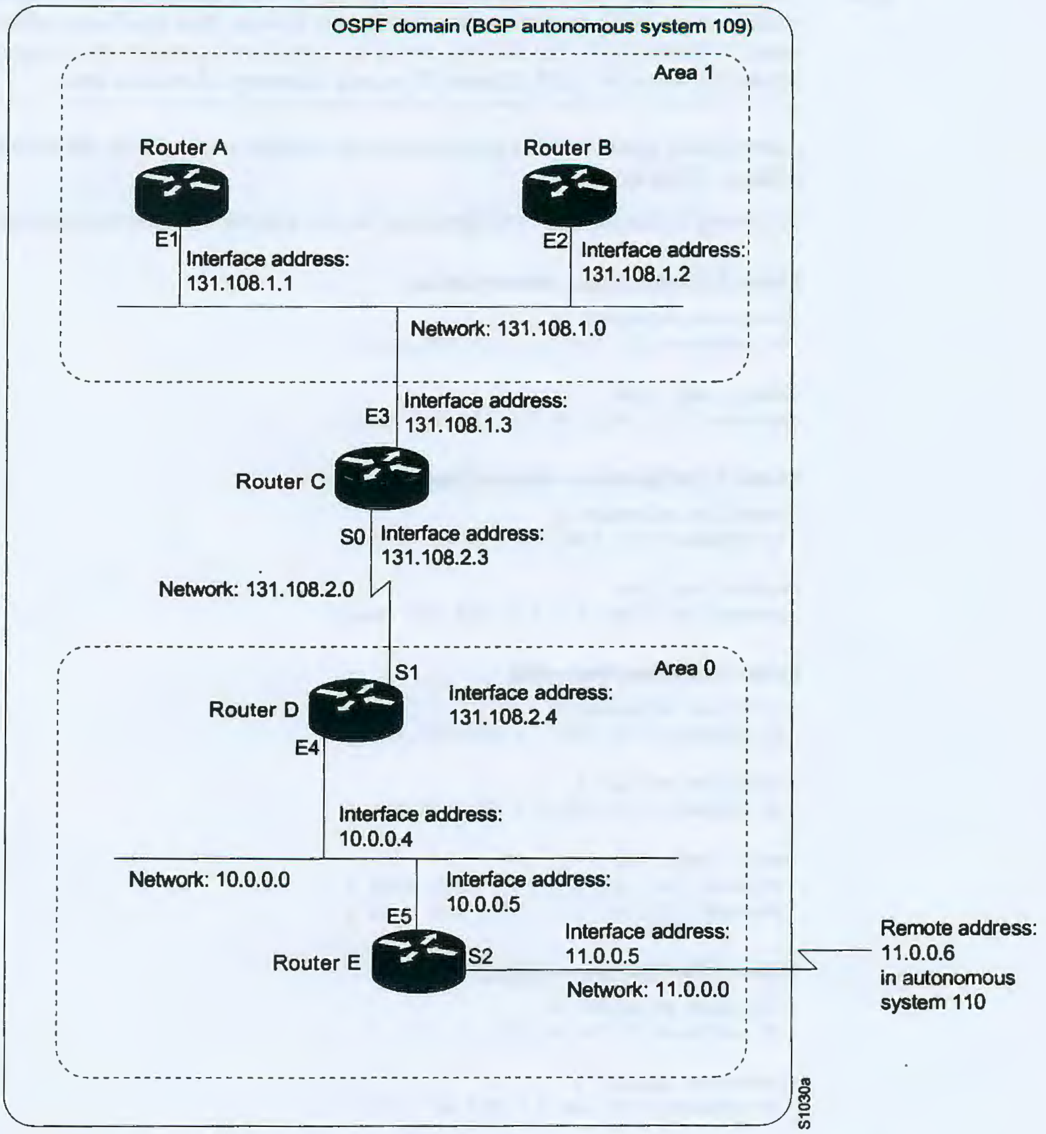
The second **network** command is evaluated next. For Area 2, the same process is then applied to all interfaces (except interface Ethernet 0). Assume that a match is determined for interface Ethernet 1. OSPF is then enabled for that interface and Ethernet 1 is attached to Area 2.

This process of attaching interfaces to OSPF areas continues for all **network** commands. Note that the last **network** command in this example is a special case. With this command, all available interfaces (not explicitly attached to another area) are attached to Area 0.

Internal Router, ABR, and ASBRs Configuration Example

Figure 61 provides a general network map that illustrates a sample configuration for several routers within a single OSPF autonomous system.

Figure 61 Example OSPF Autonomous System Network Map



In this configuration, five routers are configured in OSPF autonomous system 109:

- Router A and Router B are both internal routers within area 1.
- Router C is an OSPF ABR. Note that for Router C, area 1 is assigned to E3 and Area 0 is assigned to S0.
- Router D is an internal router in area 0 (backbone area). In this case, both **network** router configuration commands specify the same area (area 0, or the backbone area).
- Router E is an OSPF ASBR. Note that BGP routes are redistributed into OSPF and that these routes are advertised by OSPF.

7401
3

Note It is not necessary to include definitions of all areas in an OSPF autonomous system in the configuration of all routers in the autonomous system. You must only define the *directly* connected areas. In the example that follows, routes in Area 0 are learned by the routers in area 1 (Router A and Router B) when the ABR (Router C) injects summary LSAs into area 1.

Autonomous system 109 is connected to the outside world via the BGP link to the external peer at IP address 11.0.0.6.

Following is the example configuration for the general network map shown in Figure 61.

Router A Configuration—Internal Router

```
interface ethernet 1
 ip address 131.108.1.1 255.255.255.0

router ospf 109
 network 131.108.0.0 0.0.255.255 area 1
```

Router B Configuration—Internal Router

```
interface ethernet 2
 ip address 131.108.1.2 255.255.255.0

router ospf 109
 network 131.108.0.0 0.0.255.255 area 1
```

Router C Configuration—ABR

```
interface ethernet 3
 ip address 131.108.1.3 255.255.255.0

interface serial 0
 ip address 131.108.2.3 255.255.255.0

router ospf 109
 network 131.108.1.0 0.0.0.255 area 1
 network 131.108.2.0 0.0.0.255 area 0
```

Router D Configuration—Internal Router

```
interface ethernet 4
 ip address 10.0.0.4 255.0.0.0

interface serial 1
 ip address 131.108.2.4 255.255.255.0

router ospf 109
 network 131.108.2.0 0.0.0.255 area 0
 network 10.0.0.0 0.255.255.255 area 0
```

Router E Configuration—ASBR

```
interface ethernet 5
 ip address 10.0.0.5 255.0.0.0

interface serial 2
 ip address 11.0.0.5 255.0.0.0

router ospf 109
 network 10.0.0.0 0.255.255.255 area 0
 redistribute bgp 109 metric 1 metric-type 1
```

```
router bgp 109
 network 131.108.0.0
 network 10.0.0.0
 neighbor 11.0.0.6 remote-as 110
```

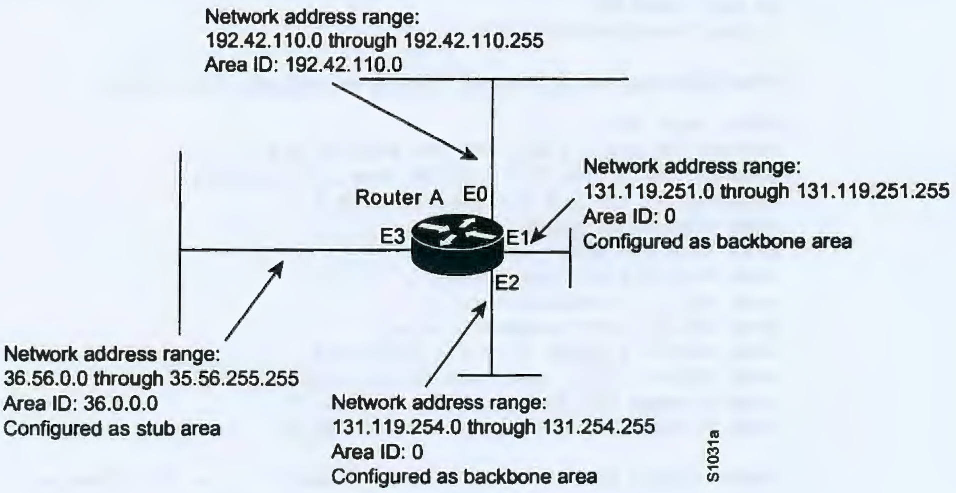
Complex OSPF Configuration Example

The following example configuration accomplishes several tasks in setting up an ABR. These tasks can be split into two general categories:

- Basic OSPF configuration
- Route redistribution

The specific tasks outlined in this configuration are detailed briefly in the following descriptions. Figure 62 illustrates the network address ranges and area assignments for the interfaces.

Figure 62 Interface and Area Specifications for OSPF Configuration Example



The basic configuration tasks in this example are as follows:

- Configure address ranges for Ethernet interface 0 through Ethernet interface 3.
- Enable OSPF on each interface.
- Set up an OSPF authentication password for each area and network.
- Assign link-state metrics and other OSPF interface configuration options.
- Create a *stub area* with area ID 36.0.0.0. (Note that the **authentication** and **stub** options of the **area** router configuration command are specified with separate **area** command entries, but can be merged into a single **area** command.)
- Specify the backbone area (area 0).

Configuration tasks associated with redistribution are as follows:

- Redistribute IGRP and RIP into OSPF with various options set (including **metric-type**, **metric**, **tag**, and **subnet**).
- Redistribute IGRP and OSPF into RIP.

The following is an example OSPF configuration:

```
interface ethernet 0
 ip address 192.42.110.201 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 1
 ip address 131.119.251.201 255.255.255.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf retransmit-interval 10
 ip ospf transmit-delay 2
 ip ospf priority 4
!
interface ethernet 2
 ip address 131.119.254.201 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 3
 ip address 36.56.0.201 255.255.0.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf dead-interval 80
```

In the following configuration, OSPF is on network 131.119.0.0:

```
router ospf 201
 network 36.0.0.0 0.255.255.255 area 36.0.0.0
 network 192.42.110.0 0.0.0.255 area 192.42.110.0
 network 131.119.0.0 0.0.255.255 area 0
 area 0 authentication
 area 36.0.0.0 stub
 area 36.0.0.0 authentication
 area 36.0.0.0 default-cost 20
 area 192.42.110.0 authentication
 area 36.0.0.0 range 36.0.0.0 255.0.0.0
 area 192.42.110.0 range 192.42.110.0 255.255.255.0
 area 0 range 131.119.251.0 255.255.255.0
 area 0 range 131.119.254.0 255.255.255.0

 redistribute igrp 200 metric-type 2 metric 1 tag 200 subnets
 redistribute rip metric-type 2 metric 1 tag 200
```

In the following configuration IGRP autonomous system 200 is on 131.119.0.0:

```
router igrp 200
 network 131.119.0.0
!
! RIP for 192.42.110
!
router rip
 network 192.42.110.0
 redistribute igrp 200 metric 1
 redistribute ospf 201 metric 1
```

Default Metric Values Redistribution Example

The following example shows a router in autonomous system 109 using both RIP and IGRP. The example advertises IGRP-derived routes using RIP and assigns the IGRP-derived routes a RIP metric of 10.

```
router rip
 default-metric 10
 redistribute igrp 109
```

Route Map Examples

The examples in this section illustrate the use of redistribution, with and without route maps. Examples from both the IP and Connectionless Network Service (CLNS) routing protocols are given.

The following example redistributes all OSPF routes into IGRP:

```
router igrp 109
 redistribute ospf 110
```

The following example redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external LSAs with a metric of 5, metric a type of type 1, and a tag equal to 1.

```
router ospf 109
 redistribute rip route-map rip-to-ospf
!
route-map rip-to-ospf permit
 match metric 1
 set metric 5
 set metric-type type1
 set tag 1
```

The following example redistributes OSPF learned routes with tag 7 as a RIP metric of 15:

```
router rip
 redistribute ospf 109 route-map 5
!
route-map 5 permit
 match tag 7
 set metric 15
```

The following example redistributes OSPF intra-area and interarea routes with next hop routers on serial interface 0 into BGP with an INTER_AS metric of 5:

```
router bgp 109
 redistribute ospf 109 route-map 10
!
route-map 10 permit
 match route-type internal
 match interface serial 0
 set metric 5
```

The following example redistributes two types of routes into the integrated IS-IS routing table (supporting both IP and CLNS). The first type is OSPF external IP routes with tag 5; these routes are inserted into Level 2 IS-IS link-state packets (LSPs) with a metric of 5. The second type is ISO-IGRP derived CLNS prefix routes that match CLNS access list 2000; these routes will be redistributed into IS-IS as Level 2 LSPs with a metric of 30.

```
router isis
 redistribute ospf 109 route-map 2
 redistribute iso-igrp nsfnet route-map 3
!
route-map 2 permit
 match route-type external
 match tag 5
 set metric 5
 set level level-2
!
route-map 3 permit
 match address 2000
 set metric 30
```

With the following configuration, OSPF external routes with tags 1, 2, 3, and 5 are redistributed into RIP with metrics of 1, 1, 5, and 5, respectively. The OSPF routes with a tag of 4 are not redistributed.

```
router rip
 redistribute ospf 109 route-map 1
!
route-map 1 permit
 match tag 1 2
 set metric 1
!
route-map 1 permit
 match tag 3
 set metric 5
!
route-map 1 deny
 match tag 4
!
route map 1 permit
 match tag 5
 set metric 5
```

Given the following configuration, a RIP learned route for network 160.89.0.0 and an ISO-IGRP learned route with prefix 49.0001.0002 will be redistributed into an IS-IS Level 2 LSP with a metric of 5:

```
router isis
 redistribute rip route-map 1
 redistribute iso-igrp remote route-map 1
!
route-map 1 permit
 match ip address 1
 match clns address 2
 set metric 5
 set level level-2
!
access-list 1 permit 160.89.0.0 0.0.255.255
 clns filter-set 2 permit 49.0001.0002...
```

The following configuration example illustrates how a route map is referenced by the **default-information** router configuration command. This type of reference is called *conditional default origination*. OSPF will originate the default route (network 0.0.0.0) with a type 2 metric of 5 if 140.222.0.0 is in the routing table.

```
route-map ospf-default permit
 match ip address 1
 set metric 5
 set metric-type type-2
!
access-list 1 140.222.0.0 0.0.255.255
!
router ospf 109
 default-information originate route-map ospf-default
```

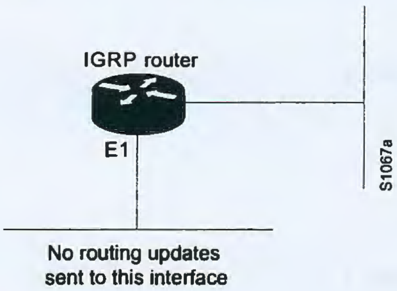
See more route map examples in the sections "BGP Route Map Examples" and "BGP Community with Route Maps Examples" in the "Configuring BGP" chapter.

Passive Interface Examples

The following example sends IGRP updates to all interfaces on network 131.108.0.0 except Ethernet interface 1. Figure 63 shows this configuration.

```
router igrp 109
 network 131.108.0.0
 passive-interface ethernet 1
```

Figure 63 Filtering IGRP Updates



In the following example, as in the first example, IGRP updates are sent to all interfaces on network 131.108.0.0 except Ethernet interface 1. However, in this case a **neighbor** router configuration command is included, which permits the sending of routing updates to specific neighbors. One copy of the routing update is generated per neighbor.

```
router igrp 109
 network 131.108.0.0
 passive-interface ethernet 1
 neighbor 131.108.20.4
```

In OSPF, hello packets are not sent on an interface that is specified as passive. Hence, the router will not be able to discover any neighbors, and none of the OSPF neighbors will be able to see the router on that network. In effect, this interface will appear as a stub network to the OSPF domain. This configuration is useful if you want to import routes associated with a connected network into the OSPF domain without any OSPF activity on that interface.

The **passive-interface** router configuration command typically is used when the wildcard specification on the **network** router configuration command configures more interfaces than is desirable. The following configuration causes OSPF to run on all subnets of 131.108.0.0:

```
interface ethernet 0
 ip address 131.108.1.1 255.255.255.0
interface ethernet 1
 ip address 131.108.2.1 255.255.255.0
interface ethernet 2
 ip address 131.108.3.1 255.255.255.0
!
router ospf 109
 network 131.108.0.0 0.0.255.255 area 0
```

If you do not want OSPF to run on 131.108.3.0, enter the following commands:

```
router ospf 109
```

```
 network 131.108.0.0 0.0.255.255 area 0
 passive-interface ethernet 2
```

Default Passive Interface Example

The following example configures the network interfaces, sets all interfaces running OSPF as passive, then enables serial interface):

```
interface Ethernet0
 ip address 172.19.64.38 255.255.255.0 secondary
 ip address 171.69.232.70 255.255.255.240
 no ip directed-broadcast
!
interface Serial0
 ip address 172.24.101.14 255.255.255.252
 no ip directed-broadcast
 no ip mroute-cache
!
interface TokenRing0
 ip address 140.10.10.4 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 ring-speed 16
!
router ospf 100
 passive-interface default
 no passive-interface Serial0
 network 140.10.10.0 0.0.0.255 area 0
 network 171.69.232.0 0.0.0.255 area 4
 network 172.24.101.0 0.0.0.255 area 4
```

Policy Routing Example

The following example provides two sources with equal access to two different service providers. Packets arriving on asynchronous interface 1 from the source 1.1.1.1 are sent to the router at 6.6.6.6 if the router has no explicit route for the destination of the packet. Packets arriving from the source 2.2.2.2 are sent to the router at 7.7.7.7 if the router has no explicit route for the destination of the packet. All other packets for which the router has no explicit route to the destination are discarded.

```
access-list 1 permit ip 1.1.1.1
access-list 2 permit ip 2.2.2.2
!
interface async 1
 ip policy route-map equal-access
!
route-map equal-access permit 10
 match ip address 1
 set ip default next-hop 6.6.6.6
route-map equal-access permit 20
 match ip address 2
 set ip default next-hop 7.7.7.7
route-map equal-access permit 30
 set default interface null0
```

NetFlow Policy Routing Example

The following example configures CEF, NetFlow, and NetFlow with flow acceleration. It also configures policy routing to verify that next hop 50.0.0.8 of the route map named test is a CDP neighbor before the router tries to policy route to it.

If the first packet is being policy routed via route map test sequence 10, the subsequent packets of the same flow always take the same route map test sequence 10, not route map test sequence 20, because they all match or pass access list 1 check. Therefore, policy routing can be flow accelerated by bypassing the access list check.

```
ip cef
ip flow-cache feature-accelerate
interface ethernet0/0/1
 ip route-cache flow
 ip policy route-map test
route-map test permit 10
 match ip address 1
 set ip precedence priority
 set ip next-hop 50.0.0.8
 set ip next-hop verify-availability
route-map test permit 20
 match ip address 101
 set interface Ethernet0/0/3
 set ip tos max-throughput
```

Key Management Examples

The following example configures a key chain named trees. In this example, the software will always accept and send willow as a valid key. The key chestnut will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The overlap allows for migration of keys or discrepancy in the set time of the router. Likewise, the key birch immediately follows chestnut, and there is a 30-minute leeway on each side to handle time-of-day differences.

```
interface ethernet 0
 ip rip authentication key-chain trees
 ip rip authentication mode md5
!
router rip
 network 172.19.0.0
 version 2
!
key chain trees
 key 1
 key-string willow
 key 2
 key-string chestnut
 accept-lifetime 13:30:00 Jan 25 1996 duration 7200
 send-lifetime 14:00:00 Jan 25 1996 duration 3600
 key 3
 key-string birch
 accept-lifetime 14:30:00 Jan 25 1996 duration 7200
 send-lifetime 15:00:00 Jan 25 1996 duration 3600
```

The following example configures a key chain named trees:

```
key chain trees
 key 1
 key-string willow
 key 2
 key-string chesnut
 accept-lifetime 00:00:00 Dec 5 1995 23:59:59 Dec 5 1995
 send-lifetime 06:00:00 Dec 5 1995 18:00:00 Dec 5 1995
!
interface Ethernet0
 ip address 172.19.104.75 255.255.255.0 secondary
 ip address 171.69.232.147 255.255.255.240
 ip rip authentication key-chain trees
 media-type 10BaseT
!
interface Ethernet1
 no ip address
 shutdown
 media-type 10BaseT
interface Fddi0
 ip address 2.1.1.1 255.255.255.0
 no keepalive
!
interface Fddi1
 ip address 3.1.1.1 255.255.255.0
 ip rip send version 1
 ip rip receive version 1
 no keepalive
!
router rip
 version 2
 network 172.19.0.0
 network 2.0.0.0
 network 3.0.0.0
```

Ap 60

Configuring Passwords and Privileges

Using passwords and assigning privilege levels is a simple way of providing terminal access control in your network.

For a complete description of the commands used in this chapter, refer to the "Password and Privileges Commands" chapter in the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the chapter "Using Cisco IOS Software."

In This Chapter

This chapter includes the following sections:

- Protecting Access to Privileged EXEC Commands
- Configuring Multiple Privilege Levels
- Recovering a Lost Enable Password
- Recovering a Lost Line Password
- Configuring Identification Support
- Passwords and Privileges Configuration Examples

Protecting Access to Privileged EXEC Commands

The following tasks provide a way to control access to the system configuration file and privileged EXEC (enable) commands:

- Setting or Changing a Static Enable Password
- Protecting Passwords with Enable Password and Enable Secret
- Setting or Changing a Line Password
- Encrypting Passwords

Setting or Changing a Static Enable Password

To set or change a static password that controls access to privileged EXEC (enable) mode, use the following command in global configuration mode:

Command	Purpose
`Router(config)# enable password password`	Establishes a new password or change an existing password for the privileged command level.

For examples of how to define enable passwords for different privilege levels, see the section "Multiple Levels of Privileges Examples" at the end of this chapter.

Protecting Passwords with Enable Password and Enable Secret

To provide an additional layer of security, particularly for passwords that cross the network or are stored on a TFTP server, you can use either the **enable password** or **enable secret** commands. Both comman accomplish the same thing; that is, they allow you to establish an encrypted password that users must enter to access enable mode (the default), or any privilege level you specify.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm. Use the **enable password** command only if you boot an older image of the Cisco IOS software, or if you boot older boot ROMs that do not recognize the **enable secret** command.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

To configure the router to require an enable password, use either of the following commands in global configuration mode:

Command	Purpose
`Router(config)# enable password [level level] {password| encryption-type encrypted-password}`	Establishes a password for a privilege command mode.
or	
`Router(config)# enable secret [level level] {password | encryption-type encrypted-password}`	Specifies a secret password, saved using a non-reversible encryption method. (If enable password and enable secret are both set, users must enter the enable secret password.)

Use either of these commands with the **level** option to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** configuration command to specify commands accessible at various levels.

If you have the **service password-encryption** command enabled, the password you enter is encrypted. When you display it with the **more system:running-config** command, it is displayed in encrypted form.

If you specify an encryption type, you must provide an encrypted password—an encrypted password you copy from another router configuration.

Note You cannot recover a lost encrypted password. You must clear NVRAM and set a new password. See the section "Recovering a Lost Enable Password" or "Recovering a Lost Line Password" in this chapter if you have lost or forgotten your password.

Setting or Changing a Line Password

To set or change a password on a line, use the following command in global configuration mode:

Command	Purpose
`Router(config)# password password`	Establishes a new password or change an existing password for the privileged command level.

Encrypting Passwords

Because protocol analyzers can examine packets (and read passwords), you can increase access security by configuring the Cisco IOS software to encrypt passwords. Encryption prevents the password from being readable in the configuration file.

To configure the Cisco IOS software to encrypt passwords, use the following command in global configuration mode:

Command	Purpose
`Router(config)# service password-encryption`	Encrypts a password.

The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and BGP neighbor passwords. The **service password-encryption** command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

Caution The **service password-encryption** command does not provide a high level of network security. If you use this command, you should also take additional network security measures.

Although you cannot recover a lost encrypted password (that is, you cannot get the original password back), you can recover from a lost encrypted password. See the section "Recovering a Lost Enable Password" or "Recovering a Lost Line Password" in this chapter if you have lost or forgotten your password.

73896

Configuring Multiple Privilege Levels

By default, the Cisco IOS software command-line interface (CLI) has two levels of access to commands: user EXEC mode (level 1) and privileged EXEC mode (level 15). However, you can configure additional levels of access to commands, called privilege levels, to meet the needs of your users while protecting the system from unauthorized access. Up to 16 privilege levels can be configured, from level 0, which is the most restricted level, to level 15, which is the least restricted level.

Access to each privilege level is enabled through separate passwords, which you specify when configuring the privilege level.

For example, if you want a certain set of users to be able to configure only certain interfaces, but not allow them access to other configuration options, you could create a separate privilege level for only specific interface configuration commands and distribute the password for that level to those users.

The following tasks describe how to configure additional levels of security:

- Setting the Privilege Level for a Command
- Changing the Default Privilege Level for Lines
- Displaying Current Privilege Levels
- Logging In to a Privilege Level

Setting the Privilege Level for a Command

To create a new privilege level and associate commands with that privilege level, use the following commands in beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **privilege** *mode* **level** *level* *command-string*	Configures the specified privilege level to allow access to the specified command.
Step 2	Router(config)# **enable secret level** *level* {0 |5} *password-string*	Sets the password for the specified privilege level. This is the password users will enter after entering the **enable** *level* command to access the specified level. • **0** indicates an unencrypted password string follows; **5** indicates an encrypted password string follows.
Step 3	Router(config)# **exit**	Exists global configuration mode and returns to EXEC mode.
Step 4	Router# do copy running-config startup-config	(Optional) Saves the configuration to the startup configuration file in NVRAM. **Note** The **do** keyword allows execution of EXEC commands in configuration mode.

Changing the Default Privilege Level for Lines

To change the default privilege level for a given line or a group of lines, use the following command in line configuration mode:

Command	Purpose
`Router(config-line)# privilege level level`	Specifies a default privilege level for a line.

Displaying Current Privilege Levels

To display the current privilege level you can access based on the password you used, use the following command in EXEC mode:

Command	Purpose
`Router# show privilege`	Displays your current privilege level.

Logging In to a Privilege Level

To log into a router at a specified privilege level, use the following command in EXEC mode:

Command	Purpose
`Router# enable level`	Logs in to a specified privilege level.

To exit to a specified privilege level, use the following command in EXEC mode:

Command	Purpose
`Router# disable level`	Exits to a specified privilege level.

Recovering a Lost Enable Password

You can restore access to enable mode on a router when the password is lost using one of the three procedures described in this section. The procedure you use depends on your router platform.

You can perform password recovery on most of the platforms without changing hardware jumpers, but all platforms require the configuration to be reloaded. Password recovery can be done only from the console port on the router. Table 26 shows which password recovery procedure to use with each router platform.

4387
6

Table 26 Platform-Specific Password Recovery Procedures

Password Recovery Procedure	Router Platform
Password Recovery Procedure 1	Cisco 2000 series Cisco 2500 series Cisco 3000 series Cisco 4000 series with 680x0 Motorola CPU Cisco 7000 series running Cisco IOS Release 10.0 or later in ROMs installed on the RP card IGS series running Cisco IOS Release 9.1 or later in ROMs
Password Recovery Procedure 2	Cisco 1003 Cisco 1600 series Cisco 2600 series Cisco 3600 series Cisco 4500 series Cisco 7100 series Cisco 7200 series Cisco 7500 series IDT Orion-based routers Cisco AS5200 and AS5300 platforms

This section includes the following sections:

- Password Recovery Process
- Password Recovery Procedure 1
- Password Recovery Procedure 2

Password Recovery Process

Both password recovery procedures involve the following basic steps:

Step 1 Configure the router to boot up without reading the configuration memory (NVRAM). This is sometimes called the test system mode.

Step 2 Reboot the system.

Step 3 Access enable mode (which can be done without a password if you are in test system mode).

Step 4 View or change the password, or erase the configuration.

Step 5 Reconfigure the router to boot up and read the NVRAM as it normally does.

Step 6 Reboot the system.

Note Some password recovery requires that a terminal issue a Break signal; you must be familiar with how your terminal or PC terminal emulator issues this signal. For example, in ProComm, the keys Alt-B by default generates the Break signal, and in a Windows terminal you press Break or CTRL-Break. A Windows terminal also allows you to define a function key as a BREAK signal. To do so, select function keys from the Terminal window and define one as Break by entering the characters **^$B** (**Shift 6**, **Shift 4**, and uppercase **B**).

Password Recovery Procedure 1

Use this procedure to recover lost passwords on the following Cisco routers:

- Cisco 2000 series
- Cisco 2500 series
- Cisco 3000 series
- Cisco 4000 series with 680x0 Motorola CPU
- Cisco 7000 series running Cisco IOS Release 10.0 or later in ROMs installed on the RP card. The router can be booting Cisco IOS Release 10.0 software in Flash memory, but it needs the actual ROMs on the processor card too.
- IGS series running Cisco IOS Release 9.1 or later in ROMs

To recover a password using Procedure 1, perform the following steps:

Step 1 Attach a terminal or PC with terminal emulation software to the console port of the router.

Step 2 Enter the **show version** command and record the setting of the configuration register. It is usually 0x2102 or 0x102.

The configuration register value is on the last line of the display. Note whether the configuration register is set to enable Break or disable Break.

The factory-default configuration register value is 0x2102. Notice that the third digit from the left in this value is 1, which disables Break. If the third digit is *not* 1, Break is enabled.

Step 3 Turn off the router, then turn it on.

Step 4 Press the **Break** key on the terminal within 60 seconds of turning on the router.

The `rommon>` prompt with no router name appears. If it does not appear, the terminal is not sending the correct Break signal. In that case, check the terminal or terminal emulation setup.

Step 5 Enter **o/r0x42** at the `rommon>` prompt to boot from Flash memory or **o/r0x41** to boot from the boot ROMs.

Note The first character is the letter o, not the numeral zero. If you have Flash memory and it is intact, 0x42 is the best setting. Use 0x41 only if the Flash memory is erased or not installed. If you use 0x41, you can only view or erase the configuration. You cannot change the password.

7385
6

Step 6 At the `rommon>` prompt, enter the initialize command to initialize the router.

This causes the router to reboot but ignore its saved configuration and use the image in Flash memory instead. The system configuration display appears.

Note If you normally use the **boot network** command, or if you have multiple images in Flash memory and you boot a non-default image, the image in Flash might be different.

Step 7 Enter **no** in response to the System Configuration Dialog prompts until the following message appears:

```
Press RETURN to get started!
```

Step 8 Press **Return**.

The `Router>` prompt appears.

Step 9 Enter **enable**.

The `Router#` prompt appears.

Step 10 Choose one of the following options:

- To view the password, if it is not encrypted, enter **more nvram:startup-config**.
- To change the password (if it is encrypted, for example), enter the following commands:

```
Router# configure memory
Router# configure terminal
Router(config)# enable secret 1234abcd
Router(config)# ctrl-z
Router# write memory
```

Note The **enable secret** command provides increased security by storing the enable secret password using a non-reversible cryptographic function; however, you cannot recover a lost password that has been encrypted.

Step 11 Enter **configure terminal** at the EXEC prompt to enter configuration mode.

Step 12 Enter **config-register** and whatever value you recorded in Step 2.

Step 13 Press **Ctrl-Z** to quit from the configuration editor.

Step 14 Enter **reload** at the privileged EXEC prompt and enter **write memory** to save the configuration.

Password Recovery Procedure 2

Use this procedure to recover lost passwords on the following routers:

- Cisco 1003
- Cisco 1600 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 3810
- Cisco 4500 series

- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- IDT Orion-Based Routers
- Cisco AS5200 and AS5300 platforms

To recover a password using Procedure 2, perform the following steps:

Step 1 Attach a terminal or PC with terminal emulation software to the console port of the router.

Step 2 Enter **show version** and record the setting of the configuration register. It is usually 0x2102 or 0x102.

The configuration register value is on the last line of the display. Note whether the configuration register is set to enable Break or disable Break.

The factory-default configuration register value is 0x2102. Notice that the third digit from the left in this value is 1, which disables Break. If the third digit is *not* 1, Break is enabled.

Step 3 Turn off the router, then turn it on.

Step 4 Press the **Break** key on the terminal within 60 seconds of turning on the router.

The `rommon>` prompt appears. If it does not appear, the terminal is not sending the correct Break signal. In that case, check the terminal or terminal emulation setup.

Step 5 Enter **confreg** at the `rommon>` prompt.

The following prompt appears:

```
Do you wish to change configuration [y/n]?
```

Step 6 Enter **yes** and press **Return**.

Step 7 Enter **no** to subsequent questions until the following prompt appears:

```
ignore system config info [y/n]?
```

Step 8 Enter **yes**.

Step 9 Enter **no** to subsequent questions until the following prompt appears:

```
change boot characteristics [y/n]?
```

Step 10 Enter **yes**.

The following prompt appears:

```
enter to boot:
```

Step 11 At this prompt, either enter **2** and press **Return** if Flash memory or, if Flash memory is erased, enter **1**. If Flash memory is erased, the Cisco 4500 must be returned to Cisco for service. If you enter **1**, you can only view or erase the configuration. You cannot change the password.

A configuration summary is displayed and the following prompt appears:

```
Do you wish to change configuration [y/n]?
```

Step 12 Enter **no** and press **Return**.

The following prompt appears:

```
rommon>
```

Step 13 Enter **reset** at the rommon prompt or, for Cisco 4500 series and Cisco 7500 series routers, power cycle the router.

Step 14 As the router boots, enter **no** to all the setup questions until the following prompt appears:

```
Router>
```

Step 15 Enter **enable** to enter enable mode.

The `Router#` prompt appears.

Step 16 Choose one of the following options:

- To view the password, if it is not encrypted, enter **more nvram:startup-config**.
- To change the password (if it is encrypted, for example), enter the following commands:

```
Router# configure memory
Router# configure terminal
Router(config)# enable secret 1234abcd
Router(config)# ctrl-z
Router# write memory
```

Note The **enable secret** command provides increased security by storing the enable secret password using a non-reversible cryptographic function; however, you cannot recover a lost password that has been encrypted.

Step 17 Enter **configure terminal** at the prompt.

Step 18 Enter **config-register** and whatever value you recorded in Step 2.

Step 19 Press **Ctrl-Z** to quit from the configuration editor.

Step 20 Enter **reload** at the prompt and enter **write memory** to save the configuration.

Recovering a Lost Line Password

If your router has the nonvolatile memory option, you can accidentally lock yourself out of enable mode if you enable password checking on the console terminal line and then forget the line password. To recover a lost line password, perform the following steps:

Step 1 Force the router into factory diagnostic mode.

See the hardware installation and maintenance publication for your product for specific information about setting the processor configuration register to factory diagnostic mode. Table 27 summarizes the hardware or software settings required by various products to set factory diagnostic mode.

Step 2 Enter **Yes** when asked if you want to set the manufacturers' addresses.

The following prompt appears:

```
TEST-SYSTEM >
```

Step 3 Enter **enable** to enter enable mode:

```
TEST-SYSTEM > enable
```

7382
ω

Step 4 Enter **more nvram:startup-config** to review the system configuration and find the password. Do not change anything in the factory diagnostic mode.

```
TEST-SYSTEM # more nvram:startup-config
```

Step 5 To resume normal operation, restart the router or reset the configuration register.

Step 6 Log in to the router with the password that was shown in the configuration file.

Note All debugging capabilities are turned on during diagnostic mode.

See the hardware installation and maintenance publication for your product for specific information about configuring the processor configuration register for factory diagnostic mode. Table 27 summarizes the hardware or software settings required by the various products to set factory diagnostic mode.

Table 27 Factory Diagnostic Mode Settings for the Configuration Register

Platform	Setting
Modular products	Set jumper in bit 15 of the processor configuration register, then restart; remove the jumper when finished.
Cisco AS5100 Cisco AS5200 Cisco AS5300 Cisco 1600 series Cisco 2500 series Cisco 3000 series Cisco 3600 series Cisco 4000 series Cisco 4500 series Cisco 7000 series Cisco 7100 series Cisco 7200 series Cisco 7500 series	Use the **config-register** command to set the processor configuration register to 0x8000, then initialize and boot the system. Use the **reload** command to restart and set the processor configuration register to 0x2102 when finished.

Configuring Identification Support

Identification support allows you to query a Transmission Control Protocol (TCP) port for identification. This feature enables an unsecure protocol, described in RFC 1413, to report the identity of a client initiating a TCP connection and a host responding to the connection. With identification support, you can connect a TCP port on a host, issue a simple text string to request information, and receive a simple text-string reply.

To configure identification support, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip identd`	Enables identification support.

Passwords and Privileges Configuration Examples

The following sections provide password and privileges configuration examples:

- Multiple Levels of Privileges Examples
- Username Examples

Multiple Levels of Privileges Examples

This section provides examples of using multiple privilege levels to specify who can access different s of commands. This section includes the following sections:

- Allowing Users to Clear Lines Examples
- Defining an Enable Password for System Operators Examples
- Disabling a Privilege Level Example

Allowing Users to Clear Lines Examples

If you want to allow users to clear lines, you can do either of the following:

- Change the privilege level for the **clear** and **clear line** commands to 1 or "ordinary user level," as follows. This allows any user to clear lines.

  ```
  privilege exec level 1 clear line
  ```

- Change the privilege level for the **clear** and **clear line** commands to level 2. To do so, use the **privilege level** global configuration command to specify privilege level 2. Then define an enable password for privilege level 2 and tell only those users who need to know what the password is.

  ```
  enable password level 2 pswd2
  privilege exec level 2 clear line
  ```

Defining an Enable Password for System Operators Examples

In the following example, you define an enable password for privilege level 10 for system operators and make **clear** and **debug** commands available to anyone with that privilege level enabled.

```
enable password level 10 pswd10
privilege exec level 10 clear line
privilege exec level 10 debug ppp chap
privilege exec level 10 debug ppp error
privilege exec level 10 debug ppp negotiation
```

The following example lowers the privilege level of the **more system:running-config** command and most configuration commands to operator level so that the configuration can be viewed by an operator. It leaves the privilege level of the **configure** command at 15. Individual configuration commands are displayed in the **more system:running-config** output only if the privilege level for a command has been lowered to 10. Users are allowed to see only those commands that have a privilege level less than or equal to their current privilege level.

```
enable password level 15 pswd15
privilege exec level 15 configure
enable password level 10 pswd10
privilege exec level 10 more system:running-config
```

Disabling a Privilege Level Example

In the following example, the **show ip route** command is set to privilege level 15. To keep all **show ip** and **show** commands from also being set to privilege level 15, these commands are specified to be privilege level 1.

```
privilege exec level 15 show ip route
privilege exec level 1 show ip
privilege exec level 1 show
```

Username Examples

The following sample configuration sets up secret passwords on Routers A, B, and C, to enable the three routers to connect to each other.

To authenticate connections between Routers A and B, enter the following commands:

On Router A:

```
username B password a-b_secret
```

On Router B:

```
username A password a-b_secret
```

To authenticate connections between Routers A and C, enter the following commands:

On Router A:

```
username C password a-c_secret
```

On Router C:

```
username A password a-c_secret
```

To authenticate connections between Routers B and C, enter the following commands:

On Router B:

```
username C password b-c_secret
```

On Router C:

```
username B password b-c_secret
```

For example, suppose you enter the following command:

```
username bill password westward
```

The system displays this command as follows:

```
username bill password 7 21398211
```

The encrypted version of the password is 21398211. The password was encrypted by the Cisco-defined encryption algorithm, as indicated by the "7."

However, if you enter the following command, the system determines that the password is already encrypted and performs no encryption. Instead, it displays the command exactly as you entered it.

```
username bill password 7 21398211
username bill password 7 21398211
```

AP GP

Configuring Voice Ports

Voice ports are found at the intersections of packet-based networks and traditional telephony networks, and they facilitate the passing of voice and call signals between the two networks. Physically, voice ports connect a router or access server to a line from a circuit-switched telephony device in a PBX or the public switched telephone network (PSTN).

Basic software configuration for voice ports describes the type of connection being made and the type of signaling to take place over this connection. Additional commands provide fine-tuning for voice quality, enable special features, and specify parameters to match those of proprietary PBXs.

This chapter includes the following sections:

Not all voice-port commands are covered in this chapter. Some are described in the "Configuring Trunk Connections and Conditioning Features" chapter or the "Configuring ISDN Interfaces for Voice" chapter in this configuration guide. The voice-port configuration commands included in this chapter are fully documented in the *Cisco IOS Voice, Video, and Fax Command Reference*.

To identify the hardware platform or software image information associated with a feature in this chapter, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the "Identifying Supported Platforms" section in the "Using Cisco IOS Software" chapter.

2377 W

Voice Port Configuration Overview

Voice ports on routers and access servers emulate physical telephony switch connections so that voice calls and their associated signaling can be transferred intact between a packet network and a circuit-switched network or device.

For a voice call to occur, certain information must be passed between the telephony devices at either end of the call, such as the devices' on-hook status, the line's availability, and whether an incoming call is trying to reach a device. This information is referred to as signaling, and to process it properly, the devices at both ends of the call segment (that is, those directly connected to each other) must use the same type of signaling.

The devices in the packet network must be configured to convey signaling information in a way that the circuit-switched network can understand. They must also be able to understand signaling information received from the circuit-switched network. This is accomplished by installing appropriate voice hardware in the router or access server and by configuring the voice ports that connect to telephony devices or the circuit-switched network.

The illustrations below show examples of voice port usage.

- In Figure 10, one voice port connects a telephone to the wide-area network (WAN) through the router.
- In Figure 11, one voice port connects to the PSTN and another to a telephone; the router acts like a small PBX.
- Figure 12 shows how two PBXs can be connected over a WAN to provide toll bypass.

Figure 10 Telephone to WAN

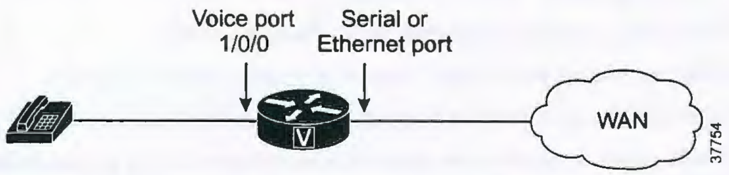


Figure 11 Telephone to PSTN

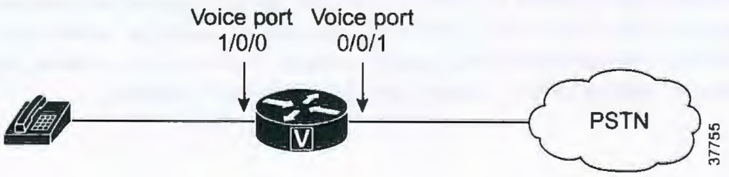
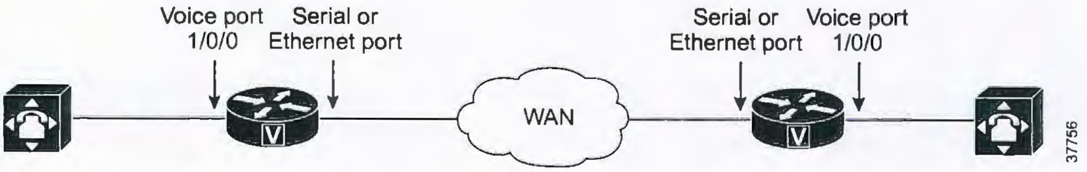


Figure 12 PBX-to-PBX over a WAN



Cisco provides a variety of Cisco IOS commands for flexibility in programming voice ports to match the physical attributes of the voice connections that are being made. Some of these connections are made using analog means of transmission, while others use digital transmission. Table 4 shows the analog and digital voice-port connection support of the router platforms discussed in this chapter.

Table 4 Analog and Digital Voice-port Support on Cisco Routers and Access Servers

Platform	Analog	Digital
Cisco 803 and 804	Yes	No
Cisco 1750	Yes	No
Cisco 2600 series	Yes	Yes
Cisco 3600 series	Yes	Yes
Cisco MC3810	Yes	Yes
Cisco AS5300	No	Yes
Cisco AS5800	No	Yes
Cisco 7200 series	No	Yes
Cisco 7500 series	No	Yes

Telephony Signaling Interfaces

Voice ports on routers and access servers physically connect the router or access server to telephony devices such as telephones, fax machines, PBXs, and PSTN central office (CO) switches. These devices may use any of several types of signaling interfaces to generate information about on-hook status, ringing, and line seizure.

The router's voice-port hardware and software need to be configured to transmit and receive the same type of signaling being used by the device with which they are interfacing so that calls can be exchanged smoothly between the packet network and the circuit-switched network.

The signaling interfaces discussed in this chapter include foreign exchange office (FXO), foreign exchange station (FXS), and receive and transmit (E&M), which are types of analog interfaces. Some digital connections emulate FXO, FXS, and E&M interfaces, and they are discussed in the second half of this chapter. It is important to know which signaling method the telephony side of the connection is using, and to match the router configuration and voice interface hardware to that signaling method.

The next three illustrations show how the different signaling interfaces are associated with different uses of voice ports. In Figure 13, FXS signaling is used for end-user telephony equipment, such as a telephone or fax machine. Figure 14 shows an FXS connection to a telephone and an FXO connection to the PSTN at the far side of a WAN; this might be a telephone at a local office going over a WAN to a router at headquarters that connects to the PSTN. In Figure 15, two PBXs are connected across a WAN by E&M interfaces. This illustrates the path over a WAN between two geographically separated offices in the same company.

7375 3

Figure 13 FXS Signaling Interfaces

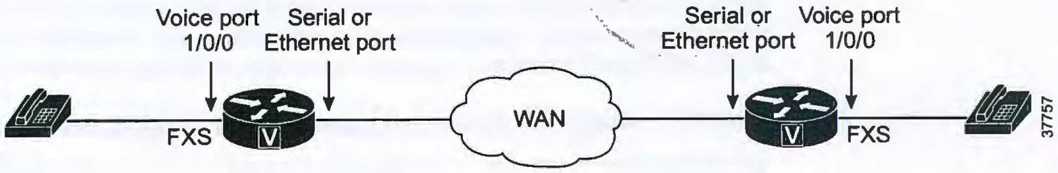


Figure 14 FXS and FXO Signaling Interfaces

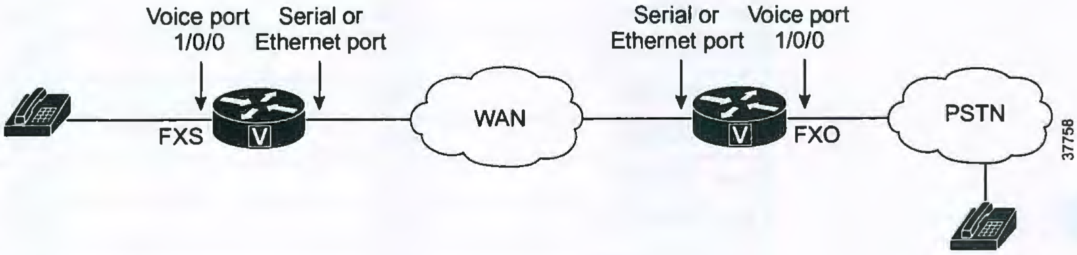
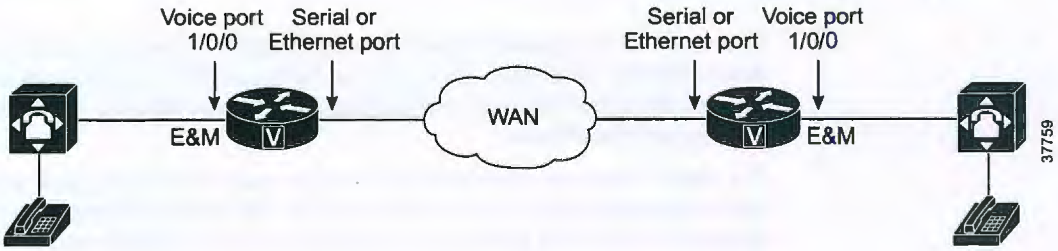


Figure 15 E&M Signaling Interfaces



FXS and FXO Interfaces

An FXS interface connects the router or access server to end-user equipment such as telephones, fax machines, or modems. The FXS interface supplies ring, voltage, and dial tone to the station and includes an RJ-11 connector for basic telephone equipment, keysets, and PBXs.

An FXO interface is used for trunk, or tie line, connections to a PSTN CO or to a PBX that does not support E&M signaling (when local telecommunications authority permits). This interface is of value for off-premise station applications. A standard RJ-11 modular telephone cable connects the FXO voice interface card to the PSTN or PBX through a telephone wall outlet.

FXO and FXS interfaces indicate on-hook or off-hook status and the seizure of telephone lines by one of two access signaling methods: loop start or ground start. The type of access signaling is determined by the type of service from the CO; standard home telephone lines use loop start, but business telephones can order ground start lines instead.

Loop-start is the more common of the access signaling techniques. When a handset is picked up (the telephone goes off-hook), this action closes the circuit that draws current from the telephone company CO and indicates a change in status, which signals the CO to provide dial tone. An incoming call is signaled from the CO to the handset by sending a signal in a standard on/off pattern, which causes the telephone to ring.

Loop-start has two disadvantages, however, that usually are not a problem on residential telephones but that become significant with the higher call volume experienced on business telephones. Loop-start signaling has no means of preventing two sides from seizing the same line simultaneously, a condition known as *glare.* Also, loop start signaling does not provide switch-side disconnect supervision for FXO calls. The telephony switch (the connection in the PSTN, another PBX, or key system) expects the router's FXO interface, which looks like a telephone to the switch, to hang up the calls it receives through its FXO port. However, this function is not built into the router for received calls; it only operates for calls originating from the FXO port.

Another access signaling method used by FXO and FXS interfaces to indicate on-hook or off-hook status to the CO is ground start signaling. It works by using ground and current detectors that allow the network to indicate off-hook or seizure of an incoming call independent of the ringing signal and allow for positive recognition of connects and disconnects. For this reason, ground start signaling is typically used on trunk lines between PBXs and in businesses where call volume on loop start lines can result in glare. See the "Disconnect Supervision Commands" section on page 84 and "FXO Supervisory Disconnect Tone Commands" section on page 87 for voice port commands that configure additional recognition of disconnect signaling.

In most cases, the default voice port command values are sufficient to configure FXO and FXS voice ports.

E&M Interfaces

Trunk circuits connect telephone switches to one another; they do not connect end-user equipment to the network. The most common form of analog trunk circuit is the E&M interface, which uses special signaling paths that are separate from the trunk's audio path to convey information about the calls. The signaling paths are known as the *E-lead* and the *M-lead*. The name *E&M* is thought to derive from the phrase *Ear* and *Mouth* or *rEceive* and *transMit* although it could also come from *Earth* and *Magnet*. The history of these names dates back to the days of telegraphy, when the CO side had a key that grounded the E circuit, and the other side had a sounder with an electromagnet attached to a battery. Descriptions such as *Ear* and *Mouth* were adopted to help field personnel determine the direction of a signal in a wire. E&M connections from routers to telephone switches or to PBXs are preferable to FXS/FXO connections because E&M provides better answer and disconnect supervision.

Like a serial port, an E&M interface has a data terminal equipment/data communications equipment (DTE/DCE) type of reference. In the telecommunications world, the *trunking* side is similar to the DCE, and is usually associated with CO functionality. The router acts as this side of the interface. The other side is referred to as the *signaling* side, like a DTE, and is usually a device such as a PBX. Five distinct physical configurations for the signaling part of the interface (Types I-V) use different methods to signal on-hook/off-hook status, as shown in Table 5. Cisco voice implementation supports E&M Types I, II, III, and V.

The physical E&M interface is an RJ-48 connector that connects to PBX trunk lines, which are classified as either two-wire or four-wire. This refers to whether the audio path is full duplex on one pair of wires (two-wire) or on two pair of wires (four-wire). A connection may be called a four-wire E&M circuit although it actually has six to eight physical wires. It is an analog connection although an analog E&M circuit may be emulated on a digital line. For more information on digital voice port configuration of E&M signaling, see the "DS0 Groups on Digital T1/E1 Voice Ports" section on page 72.

7372
E

PB?s built by different manufacturers can indicate on-hook/off-hook status and telephone line seizure on the E&M interface by using any of three types of access signaling that are as follows:

- Immediate-start is the simplest method of E&M access signaling. The calling side seizes the line by going off-hook on its E-lead and sends address information as dual-tone multifrequency (DTMF) digits (or as dialed pulses on Cisco 2600 series routers and Cisco 3600 series routers) following a short, fixed-length pause.
- Wink-start is the most commonly used method for E&M access signaling, and is the default for E&M voice ports. Wink-start was developed to minimize glare, a condition found in immediate-start E&M, in which both ends attempt to seize a trunk at the same time. In wink-start, the calling side seizes the line by going off-hook on its E-lead, then waits for a short temporary off-hook pulse, or "wink," from the other end on its M-lead before sending address information. The switch interprets the pulse as an indication to proceed and then sends the dialed digits as DTMF or dialed pulses.
- In delay-dial signaling, the calling station seizes the line by going off-hook on its E-lead. After a timed interval, the calling side looks at the status of the called side. If the called side is on-hook, the calling side starts sending information as DTMF digits; otherwise, the calling side waits until the called side goes on-hook and then starts sending address information.

Table 5 E&M Wiring and Signaling Methods

E&M Type	E-Lead Configuration	M-Lead Configuration	Signal Battery Lead Configuration	Signal Ground Lead Configuration
I	Output, relay to ground	Input, referenced to ground	—	—
II	Output, relay to SG	Input, referenced to ground	Feed for M, connected to –48V	Return for E, galvanically isolated from ground
III	Output, relay to ground	Input, referenced to ground	Connected to –48V	Connected to ground
V	Output, relay to ground	Input, referenced to –48V	—	—

Analog Voice Ports Configuration Task List

Analog voice port interfaces connect routers in packet-based networks to analog two-wire or four-wire analog circuits in telephony networks. Two-wire circuits connect to analog telephone or fax devices, and four-wire circuits connect to PBXs. Typically, connections to the PSTN CO are made with digital interfaces.

This section describes how to configure analog voice ports and covers the following topics:

- Configuring Codec Complexity for Analog Voice Ports on the Cisco MC3810 with High-Performance Compression Modules, page 47
- Configuring Basic Parameters on Analog FXO, FXS, or E&M Voice Ports, page 48
- Configuring Analog Telephone Connections on Cisco 803 and 804 Routers, page 52

Three other sections later in the chapter provide help with fine-tuning and troubleshooting:

- Fine-Tuning Analog and Digital Voice Ports, page 80
- Verifying Analog and Digital Voice-Port Configurations, page 99
- Troubleshooting Analog and Digital Voice Port Configurations, page 110

Prerequisites for Configuring Analog Voice Ports

- Obtain two- or four-wire line service from your service provider or from a PBX.
- Complete your company's dial plan.
- Establish a working telephony network based on your company's dial plan.
- Install at least one other network module or WAN interface card to provide the connection to the network LAN or WAN.
- Establish a working IP and Frame Relay or ATM network. For more information about configuring IP, refer to the *Cisco IOS IP Configuration Guide*, Release 12.2.
- Install appropriate voice processing and voice interface hardware on the router. See the "Configuring Platform-Specific Analog Voice Hardware" section on page 45.

Preparing to Configure Analog Voice Ports

Before configuring an analog voice port, assemble the following information about the telephony connection that the voice port will be making. If connecting to a PBX, it is important to understand the PBX's wiring scheme and timing parameters. This information should be available from your PBX vendor or the reference manuals that accompany your PBX.

- Telephony signaling interface: FXO, FXS, or E&M
- Locale code (usually the country) for call progress tones
- If FXO, type of dialing: DTMF (touch-tone) or pulse
- If FXO, type of start signal: loop-start or ground-start
- If E&M, type: I, II, III, or V
- If E&M, type of line: two-wire or four-wire
- If E&M, type of start signal: wink, immediate, delay-dial

Table 6 should help you determine which hardware and configuration instructions are appropriate for your situation. Table 7 on page 44 shows slot and port numbering, which differs for each of the voice-enabled routers. More current information may be available in the release notes that accompany the Cisco IOS software you are using.

Table 6 Analog Voice Port Configurations

Telephony Signaling Interface	Router Platform	Voice Hardware Required	Section Containing Voice Port Configuration Instructions
End user: telephone or fax	Cisco 803 Cisco 804	—	"Configuring Analog Telephone Connections on Cisco 803 and 804 Routers"
FXO	Cisco 1750 Cisco 2600 series Cisco 3600 series	VIC-2FXO, VIC-2FXO-EU	"Configuring Basic Parameters on Analog FXO, FXS, or E&M Voice Ports"
	Cisco MC3810	MC3810-AVM6 MC3810-APM-FXO	
FXS	Cisco 1750 Cisco 2600 series Cisco 3600 series	VIC-2FXS	
	Cisco MC3810	MC3810-AVM6 MC3810-APM-FXS	
E&M	Cisco 1750 Cisco 2600 series Cisco 3600 series	VIC-2E/M	
	Cisco MC3810	MC3810-AVM6 MC3810-APM-EM	

Table 7 Analog Voice Slot/Port Designations

Router Platform	Voice Hardware	Chassis Slot Numbers	Voice NM Slot Numbers	Voice Port Numbers
Cisco 803, 804	Analog POTS	—	—	—
Cisco 1750	Analog VIC	0 to 1	—	0 to 1
Cisco 2600 series	Voice/fax network module with two-port VIC	Varies, based on router	1	0 to 1
Cisco 3600 series	Voice/fax network module with two-port voice over interface cards (VICs)	1	3620: 0 to 1 3640: 0 to 3 3660: 1 to 6	0 to 1
Cisco MC3810	Analog voice module (AVM)	1	—	1 to 6

7369

Configuring Platform-Specific Analog Voice Hardware

This section describes the general types of analog voice port hardware available for the router platforms included in this chapter:

- Cisco 800 Series Routers, page 45
- Cisco 1750 Modular Router, page 45
- Cisco 2600 Series and Cisco 3600 Series Routers, page 46
- Cisco MC3810 Multiservice Concentrator, page 46

Note For current information about supported hardware, see the release notes for the platform and Cisco IOS release being used.

Cisco 800 Series Routers

Cisco 803 and Cisco 804 routers support data and voice applications. The data applications on these routers are implemented through the ISDN port, and the voice applications are implemented with ISDN Basic Rate Interface (BRI) through the telephone ports. If a Cisco 803 or 804 router is being used, connect two devices, such as an analog touch-tone telephone, fax machine, or modem through two fixed telephone ports, the gray PHONE 1 and PHONE 2 ports that have RJ-11 connectors. Each device is connected to basic telephone services through the ISDN line.

For more information, refer to the *Cisco 800 Series Routers Hardware Installation Guide.*

Cisco 1750 Modular Router

The Cisco 1750 modular router provides Voice over IP (VoIP) functionality and can carry voice traffic (for example, telephone calls and faxes) over an IP network. To make a voice connection, the router must have a supported VIC installed. The Cisco 1750 router supports two slots for either WAN interface cards (WICs) or VICs and supports one VIC-only slot. For analog connections, two-port VICs are available to support FXO, FXS, and E&M signaling. VICs provide direct connections to telephone equipment (analog phones, analog fax machines, key systems, or PBXs) or to a PSTN.

For more information, refer to the *Cisco 1750 Voice-over-IP Quick Start Guide.*

4368
ε

Cisco 2600 Series and Cisco 3600 Series Routers

The Cisco 2600 and 3600 series routers are modular, multifunction platforms that combine dial access, routing, local area network-to-local area network (LAN) services, and multiservice integration of voice, video, and data in the same device.

Voice network modules installed in Cisco 2600 series or Cisco 3600 series routers convert telephone voice signals into data packets that can be transmitted over an IP network. The voice network modules have no connectors; VICs installed in the network modules provide connections to the telephone equipment or network. VICs work with existing telephone and fax equipment and are compatible with H.323 standards for audio and video conferencing.

The Cisco 2600 series router can house one network module. In the Cisco 3600 series, the Cisco 3620 router has slots for up to two network modules; the Cisco 3640 router has slots for up to four network modules; and the Cisco 3660 router has slots for up to six network modules. (Typically, one of the slots is used for LAN connectivity.)

For analog telephone connections, low-density voice/fax network modules that contain either one or two VIC slots are installed in the network module slots. Each VIC is specific to a particular telephone signaling interface (FXS, FXO, or E&M); therefore, the VIC determines the type of signaling on that module.

For more information, refer to the following:

- *Cisco 2600 Series Hardware Installation Guide*
- *Cisco 3600 Series Hardware Installation Guide*
- *Cisco Network Module Hardware Installation Guide*

Cisco MC3810 Multiservice Concentrator

To support analog voice circuits, a Cisco MC3810 multiservice concentrator must be equipped with an AVM, which supports six analog voice ports. By installing specific signaling modules known as analog personality modules (APMs), the analog voice ports may be equipped for the following signaling types in various combinations: FXS, FXO, and E&M. For FXS, the analog voice ports use an RJ-11 connector interface to connect to analog telephones or fax machines (two-wire) or to a key system (four-wire). For FXO, the analog voice ports use an RJ-11 physical interface to connect to a CO trunk. For E&M connections, the analog voice ports use an RJ-1CX physical interface to connect to an analog PBX (two-wire or four-wire).

Optional high-performance voice compression modules (HCMs) can replace standard voice compression modules (VCMs) to operate according to the voice compression coding algorithm (codec) specified when the Cisco MC3810 concentrator is configured. The HCM2 provides four voice channel at high codec complexity and eight channels at medium complexity. The HCM6 provides 12 voice channels at high complexity and 24 channels at medium complexity. One or two HCMs can be installed in a Cisco MC3810 multiservice concentrator, but an HCM may not be combined with a VCM in one chassis.

For more information, refer to the *Cisco MC3810 Multiservice Concentrator Hardware Installation Guide*.

Note For current information about supported hardware, see the release notes for the platform and Cisco IOS release being used.

Configuring Codec Complexity for Analog Voice Ports on the Cisco MC3810 with High-Performance Compression Modules

The term *codec* stands for *coder-decoder.* A codec is a particular method of transforming analog voice into a digital bit stream (and vice versa) and also refers to the type of compression used. Several different codecs have been developed to perform these functions, and each one is known by the number of the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) standard in which it is defined. For example, two common codecs are the G.711 and the G.729 codecs. The various codecs use different algorithms to encode analog voice into digital bit-streams and have different bit rates, frame sizes, and coding delays associated with them. The codecs also differ in the amount of perceived voice quality they achieve. Specialized hardware and software in the digital signal processors (DSPs) perform codec transformation and compression functions, and different DSPs may offer different selections of codecs.

Select the same type of codec as the one that is used at the other end of the call. For instance, if a call was coded with a G.729 codec, it must be decoded with a G.729 codec. Codec choice is configured on dial peers. For more information, see the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter in this configuration guide.

Codec complexity refers to the amount of processing power that a codec compression technique requires: some require more processing power than others. Codec complexity affects call density, which is the number of calls that can take place on the DSP interfaces, which can be HCMs, port adapter DSP farms, or voice cards, depending on the type of router (in this case, the Cisco MC3810 multiservice concentrator). The greater the codec complexity, the fewer the calls that can be handled.

Codec complexity is either medium or high. The difference between medium- and high-complexity codecs is the amount of CPU power necessary to process the algorithm and, therefore, the number of voice channels that can be supported by a single DSP. All medium-complexity codecs can also be run in high-complexity mode, but fewer (usually half as many) channels will be available per DSP.

For details on the number of calls that can be handled simultaneously using each of the codec standards, refer to the entries for the **codec** and **codec complexity** commands in the *Cisco IOS Voice, Video, and Fax Command Reference*.

On a Cisco MC3810 concentrator, only a single codec complexity setting is used, even when two HCMs are installed. The value that is specified in this task affects the choice of codecs available when the **codec** dial-peer configuration command is configured. See the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter in this configuration guide.

Note On the Cisco MC3810 with high-performance compression modules, check the DSP voice channel activity with the **show voice dsp** command. If any DSP voice channels are in the busy state, the codec complexity cannot be changed. When all the DSP channels are in the idle state, changes can be made to the codec complexity selection.

7366 E

To configure codec complexity on the Cisco MC3810 multiservice concentrator using HCMs, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# show voice dsp`	Checks the DSP voice channel activity. If any DSP voice channels are in the busy state, the codec complexity cannot be changed. When all the DSP channels are in the idle state, continue to Step 2.
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# voice-card 0`	Enters voice-card configuration mode and specifies voice card 0.
Step 4	`Router(config-voicecard)# codec complexity {high | medium}`	(For analog voice ports) Specifies codec complexity based on the codec standard being used. This setting restricts the codecs available in dial peer configuration. All voice cards in a router must use the same codec complexity setting. The keywords are as follows: • **high**—Specifies two voice channels encoded in any of the following formats: G.711ulaw, G.711alaw, G.723.1(r5.3), G.723.1 Annex A(r5.3), G.723.1(r6.3), G.723.1 Annex A(r6.3), G.726(r16), G.726(r24), G.726(r32), G.728, G.729, G.729 Annex B, and fax relay. • **medium**—(default) Specifies four voice channels encoded in any of the following formats: G.711ulaw, G.711alaw, G.726(r16), G.726(r24), G.726(r32), G.729 Annex A, G.729 Annex B with Annex A, and fax relay. **Note** If two HCMs are installed, this command configures both HCMs at once.

Configuring Basic Parameters on Analog FXO, FXS, or E&M Voice Ports

This section describes commands for basic analog voice port configuration. All the data recommended in the "Preparing to Configure Analog Voice Ports" section on page 43 should be gathered before starting this procedure.

If configuring a Cisco MC3810 multiservice concentrator that has HCMs, codec complexity should also be configured, following the steps in the "Configuring Codec Complexity for Analog Voice Ports on the Cisco MC3810 with High-Performance Compression Modules" section on page 47.

Note If you have a Cisco MC3810 multiservice concentrator or Cisco 3660 router, the **compand-type a-law** command must be configured on the analog ports only. The Cisco 2660, 3620, and 3640 routers do not require the configuration of th **compand-type a-law** command, however, if you request a list of commands, the **compand-type a-law** command will display.

In addition to the basic voice port parameters described in this section, there are commands that allow voice port configurations to be fine tuned. In most cases, the default values for fine-tuning commands are sufficient for establishing FXO and FXS voice port configurations. E&M voice ports are more likely to require some configuration. If it is necessary to change some of the voice port values to improve voice quality or to match parameters on proprietary PBXs to which you are connecting, use the commands in the current section and also in the "Fine-Tuning Analog and Digital Voice Ports" section on page 80.

After the voice-port has been configured, make sure that the ports are operational by following the steps described in the following sections:

- Verifying Analog and Digital Voice-Port Configurations, page 99
- Troubleshooting Analog and Digital Voice Port Configurations, page 110

For more information on these and other voice port commands, see the *Cisco IOS Voice, Video, and Fax Command Reference*.

Note The commands, keywords, and arguments that you are able to use may differ slightly from those presented here, based on your platform, Cisco IOS release, and configuration. When in doubt, use Cisco IOS command help (**command ?**) to determine the syntax choices that are available.

To configure basic analog voice port parameters on Cisco 1750, Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 routers, use the following commands beginning in global configuration mode:

	Command	Purpose

Step 1	**Cisco 1750 and MC3810**
	`Router(config)# voice-port slot/port`
	Cisco 2600 and 3600 series
	`Router(config)# voice-port slot/subunit/port`
		Enters voice-port configuration mode.
		The arguments are as follows:
		• *slot*—Specifies the number of the router slot where the voice network module is installed (Cisco 2600 and Cisco 3600 series routers) or the router slot number where the analog voice module is installed (Cisco MC3810 multiservice concentrator).
		• *port*—Indicates the voice port. Valid entries are 0 or 1.
		• *subunit*—Specifies the location of the VIC.
		Note The slash must be entered between *slot* and *port*.
		Valid entries vary by router platform; see Table 7 on page 44 or enter the **show voice port summary** command for available values.

Step 2	**FXO or FXS** `Router(config-voiceport)# signal {loop-start | ground-start}`	Selects the access signaling type to match that of the telephony connection you are making. The keywords are as follows: • **loop-start**—(default) Uses a closed circuit to indicate off-hook status; used for residential loops. • **ground-start**—Uses ground and current detectors; preferred for PBXs and trunks.

	Command	Purpose
	E&M `Router(config-voiceport)# signal {wink-start | immediate-start | delay-dial}`	The keywords are as follows: • **wink-start**—(default) Indicates that the calling side seizes the line, then waits for a short off-hook *wink* from the called side before proceeding. • **immediate-start**—Indicates that the calling side seizes the line and immediately proceeds; used for E&M tie trunk interfaces. • **delay-dial**—Indicates that the calling side seizes the line and waits, then checks to determine whether the called side is on-hook before proceeding; if not, it waits until the called side is on-hook before sending digits. Used for E&M tie trunk interfaces. **Note** Configuring the **signal** keyword for one voice port on a Cisco 2600 or 3600 series router VIC changes the signal value for both ports on the VIC.
Step 3	`Router(config-voiceport)# cptone locale`	Selects the two-letter locale for the voice call progress tones and other locale-specific parameters to be used on this voice port. Cisco routers comply with the ISO 3166 locale name standards. To see valid choices, enter a question mark (?) following the **cptone** command. The default is **us**.
Step 4	`Router(config-voiceport)# dial-type {dtmf | pulse}`	(FXO only) Specifies the dialing method for outgoing calls.
Step 5	`Router(config-voiceport)# operation {2-wire | 4-wire}`	(E&M only) Specifies the number of wires used for voice transmission at this interface (the audio path only, not the signaling path). The default is 2-wire.
Step 6	`Router(config-voiceport)# type {1 | 2 | 3 | 5}`	(E&M only) Specifies the type of E&M interface to which this voice port is connecting. See Table 5 on page 42 for an explanation of E&M types. The default is 1.

Step 7	**Cisco 1750 Router and 2600 and 3600 Series Routers**
	`Router(config-voiceport)# ring frequency {25 | 50}`
	Cisco MC3810 Multiservice Concentrator
	`Router(config-voiceport)# ring frequency {20 | 30}`
		(FXS only) Selects the ring frequency, in hertz, used on the FXS interface. This number must match the connected telephony equipment and may be country-dependent. If not set properly, the attached telephony device may not ring or it may buzz.
		The keyword default is 25 on the Cisco 1750 router, 2600 and 3600 series routers; and 20 on the Cisco MC3810 multiservice concentrator.

	Command	Purpose
Step 8	`Router(config-voiceport)# ring number number`	(FXO only) Specifies the maximum number of rings to be detected before an incoming call is answered by the router. The default is 1.
Step 9	`Router(config-voiceport)# ring cadence {[pattern01 | pattern02 | pattern03 | pattern04 | pattern05 | pattern06 | pattern07 | pattern08 | pattern09 | pattern10 | pattern11 | pattern12] | [define pulse interval]}`	(FXS only) Specifies an existing pattern for ring, or it defines a new one. Each pattern specifies a ring-pulse time and a ring-interval time. The keywords and arguments are as follows: • **pattern01** through **pattern12** name pre-set ring cadence patterns. Enter **ring cadence ?** to see ring pattern explanations. • **define** *pulse interval* specifies a user-defined pattern: *pulse* is a number (one or two digits, from 1 to 50) specifying ring pulse (on) time in hundreds of milliseconds, and *interval* is a number (one or two digits from 1 to 50) specifying ring interval (off) time in hundreds of milliseconds. The default is the pattern specified by the cptone locale that has been configured.
Step 10	`Router(config-voiceport)# description string`	Attaches a text string to the configuration that describes the connection for this voice port. This description appears in various displays and is useful for tracking the purpose or use of the voice port. The *string* argument is a character string from 1 to 255 characters in length. The default is that there is no text string (describing the voice port) attached to the configuration.
Step 11	`Router(config-voiceport)# no shutdown`	Activates the voice port. If a voice port is not being used, shut the voice port down with the **shutdown** command.

7.362)

Configuring Analog Telephone Connections on Cisco 803 and 804 Routers

Multiple devices (analog telephone, fax machine, or modem) can be connected to a Cisco 803 or 804 telephone port. The number of devices that can be connected depends on the ringer equivalent number (REN) of each device that is to be connected. (The REN can usually be found on the bottom of a device.) The REN of the router telephone port is 5, so if the REN of each device to be connected is 1, a maximum of five devices can be connected to that particular telephone port.

These routers support touch-tone analog telephones only; they do not support rotary telephones.

To configure standard features for analog telephone connections on Cisco 803 and 804 routers, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# pots country country`	Specifies the country to use for country-specific default settings for physical characteristics. Enter **pots country ?** for a list of supported countries and the codes to enter. A default country is not defined.
Step 2	`Router(config)# pots line-type {type1 | type2 | type3}`	(Optional) Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router. The keywords are as follows: • **type1**—Specifies the resistance used for the POTS connection, typically 600 ohms. • **type2**—Specifies the resistance used for the POTS connection, typically 900 ohms. • **type3**—Specifies the resistance used for the POTS connection, typically 300/400 ohms. The default depends on the country chosen in the **pots country** command.
Step 3	`Router(config)# pots dialing-method {overlap | enblock}`	(Optional) Specifies how the router collects and sends digits dialed on connected telephones, fax machines, or modems. The keywords are as follows: • **overlap**—Tells the router to send each digit dialed in a separate message. • **enblock**—Tells the router to collect all digits dialed and to send the digits in one message. The default depends on the country chosen in the **pots country** command.

4.361

	Command	Purpose
Step 4	`Router(config)# pots disconnect-supervision {osi | reversal}`	(Optional) Specifies how the router notifies the connected telephones, fax machines, or modems when the calling party has disconnect. The keywords are as follows: • **osi**—(open switching interval) Specifies the duration for which DC voltage applied between tip and ring conductors of a telephone port is removed. • **reversal**—Specifies the polarity reversal of the tip and ring conductors of a telephone port. The default depends on the country chosen in the **pots country** command.
Step 5	`Router(config)# pots encoding {alaw | ulaw}`	(Optional) Specifies the pulse code modulation (PCM) encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router. The keywords are as follows: • **alaw**—Specifies the ITU-T PCM encoding scheme used to represent analog voice samples as digital values. • **ulaw**—Specifies the North American PCM encoding scheme used to represent analog voice samples as digital values. The default depends on the country chosen in the **pots country** command.
Step 6	`Router(config)# pots tone-source {local | remote}`	(Optional) Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router. The keywords are as follows: • **local**—(default) Specifies that the router supplies the tones. • **remote**—Specifies that the telephone switch supplies the tones.
Step 7	`Router(config)# pots ringing-freq {20Hz | 25Hz | 50Hz}`	(Optional) Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring. The keywords are as follows: • **20Hz**—Indicates that connected devices ring at 20 Hz. • **25Hz**—Indicates that connected devices ring at 25 Hz. • **50Hz**—Indicates that connected devices ring at 50 Hz. The default depends on the country chosen in the **pots country** command.

7.360

	Command	Purpose
Step 8	`Router(config)# `**`pots disconnect-time`** *`interval`*	(Optional) Specifies the interval at which the disconnect method is applied if connected telephones, fax machines, or modems fail to detect that a calling party has disconnected. The *interval* argument is the number of milliseconds of the interval and ranges from 50 to 2000. The default depends on the country chosen in the **pots country** command.
Step 9	`Router(config)# `**`pots silence-time`** *`seconds`*	(Optional) Specifies the interval of silence after a calling party disconnects. The *seconds* argument is the number of seconds of the interval and ranges from 0 to 10. The default depends on the country chosen in the **pots country** command.
Step 10	`Router(config)# `**`pots distinctive-ring-guard-time`** *`milliseconds`*	(Optional) Specifies the delay after which a telephone port can be rung after a previous call is disconnected. The *milliseconds* argument is the number of milliseconds of the delay and ranges from 0 to 1000. The default depends on the country chosen in the **pots country** command.

Verifying Analog Telephone Connections on Cisco 803 and 804 Routers

After configuring analog telephone connections, perform the following steps to verify proper operation:

Step 1 Pick up the handset of an attached telephony device and check for a dial tone.

Step 2 Review the configuration using the **show pots status** command, which displays settings of physical characteristics and other information on telephone interfaces.

```
Router# show pots status

POTS Global Configuration:
 Country: United States
  Dialing Method: Overlap, Tone Source: Remote, CallerId Support: YES
  Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
  Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
  Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
  TX Gain: 6dB, RX Loss: -6dB,
  Filter Mask: 6F
  Adaptive Cntrl Mask: 0
POTS PORT: 1
  Hook Switch Finite State Machine:
   State: On Hook, Event: 0
   Hook Switch Register: 10, Suspend Poll: 0
  CODEC Finite State Machine
   State: Idle, Event: 0
  Connection: None, Call Type: Two Party, Direction: Rx only
  Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
  Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
  Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
  TX Gain: 6dB, RX Loss: -6dB,
  Filter Mask: 6F
  Adaptive Cntrl Mask: 0
  CODEC Registers:
   SPI Addr: 2, DSLAC Revision: 4
   SLIC Cmd: 0D, TX TS: 00, RX TS: 00
   Op Fn: 6F, Op Fn2: 00, Op Cond: 00
   AISN: 6D, ELT: B5, EPG: 32 52 00 00
   SLIC Pin Direction: 1F
  CODEC Coefficients:
   GX: A0 00
   GR: 3A A1
   Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
   B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
   X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
   R: 01 11 01 90 01 90 01 90 01 90 01 90
   GZ: 60
  ADAPT B: 91 B2 8F 62 31
 CSM Finite State Machine:
   Call 0 - State: idle, Call Id: 0x0
    Active: no
   Call 1 - State: idle, Call Id: 0x0
    Active: no
   Call 2 - State: idle, Call Id: 0x0
    Active: no
 POTS PORT: 2
   Hook Switch Finite State Machine:
    State: On Hook, Event: 0
    Hook Switch Register: 20, Suspend Poll: 0
   CODEC Finite State Machine:
    State: Idle, Event: 0
    Connection: None, Call Type: Two Party, Direction: Rx only
    Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
    Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 mse
  Disconnect timer: 1000msec,Disconnect Silence timer: 5 sec
   TX Gain: 6dB, RX Loss: -6dB,
   Filter Mask: 6F
   Adaptive Cntrl Mask: 0
 CODEC Registers:
   SPI Addr: 3, DSLAC Revision: 4
   SLIC Cmd: 0D, TX TS: 00, RX TS: 00
   Op Fn: 6F, Op Fn2: 00, Op Cond: 00
   AISN: 6D, ELT: B5, EPG: 32 52 00 00
   SLIC Pin Direction: 1F
 CODEC Coefficients:
   GX: A0 00
   GR: 3A A1
   Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
   B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
   X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
   R: 01 11 01 90 01 90 01 90 01 90 01 90
   GZ: 60
  ADAPT B: 91 B2 8F 62 31
 CSM Finite State Machine:
   Call 0 - State: idle, Call Id: 0x0
    Active: no
   Call 1 - State: idle, Call Id: 0x0
    Active: no
   Call 2 - State: idle, Call Id: 0x0
    Active: no
Time Slot Control: 0
```

7.358

Troubleshooting Tip for Cisco 803 and 804 Routers

Check to ensure that all cables are securely connected.

Configuring Digital Voice Ports

The digital voice port commands discussed in this section configure channelized T1 or E1 connections; for information on ISDN connections, see "Configuring ISDN Interfaces for Voice" in this configuration guide.

The T1 or E1 lines that connect a telephony network to the digital voice ports on a router or access server contain channels for voice calls; a T1 line contains 24 full-duplex channels or *timeslots*, and an E1 line contains 30. The signal on each channel is transmitted at 64 kbps, a standard known as digital signal 0 (DS0); the channels are known as DS0 channels. The **ds0-group** command creates a logical voice port (a DS0 group) from some or all of the DS0 channels, which allows you to address those channels easily, as a group, in voice-port configuration commands.

Digital voice ports are found at the intersection of a packet voice network and a digital, circuit-switched telephone network. The digital voice port interfaces that connect the router or access server to T1 or E1 line pass voice data and signaling between the packet network and the circuit-switched network.

Signaling is the exchange of information about calls and connections between two ends of a communication path. For instance, signaling communicates to the call's end points whether a line is idle or busy, whether a device is on-hook or off-hook, and whether a connection is being attempted. An end point can be a CO switch, a PBX, a telephony device such as a telephone or fax machine, or a voice-equipped router acting as a gateway. There are two aspects to consider about signaling on digital lines: one aspect is the actual information about line and device states that is transmitted, and the second aspect is the method used to transmit the information on the digital lines.

The actual information about line and device states is communicated over digital lines using signaling methods that emulate the methods used in analog circuit-switched networks: FXS, FXO, and E&M.

The method used to transmit the information describes the way that the emulated analog signaling is transmitted over digital lines, which may be *common-channel signaling* (CCS) or *channel-associated signaling* (CAS). CCS sends signaling information down a dedicated channel and CAS takes place within the voice channel itself. This chapter describes CAS signaling, which is sometimes called *robbed-bit signaling* because user bandwidth is *robbed* by the network for signaling. A bit is taken from every sixth frame of voice data to communicate on- or off-hook status, wink, ground start, dialed digits, and other information about the call.

In addition to setting up and tearing down calls, CAS provides the receipt and capture of dialed number identification (DNIS) and automatic number identification (ANI) information, which are used to suppo authentication and other functions. The main disadvantage of CAS signaling is its use of user bandwidth to perform these signaling functions.

For signaling to pass between the packet network and the circuit-switched network, both networks must use the same type of signaling. The voice ports on Cisco routers and access servers can be configured to match the signaling of most COs and PBXs, as explained in this chapter.

This section discusses the following topics:

- Prerequisites for Configuring Digital Voice Ports, page 57
- Preparing Information to Configure Digital Voice Ports, page 58
- Platform-Specific Digital Voice Hardware, page 60
- Configuring Basic Parameters on Digital T1/E1 Voice Ports, page 63

Prerequisites for Configuring Digital Voice Ports

Digital T1 or E1 packet voice capability requires specific service, software, and hardware:

- Obtain T1 or E1 service from the service provider or from your PBX.
- Create your company's dial plan.
- Establish a working telephony network based on your company's dial plan.
- Establish a connection to the network LAN or WAN.
- Set up a working IP and Frame Relay or ATM network. For more information about configuring IP, refer to the *Cisco IOS IP Configuration Guide*, Release 12.2.
- Install appropriate voice processing and voice interface hardware on the router. See the "Platform-Specific Digital Voice Hardware" section on page 60.
- (Cisco 2600 and 3600 series routers) For digital T1 packet voice trunk network modules, install Cisco IOS Release 12.0(5)XK, 12.0(7)T, 12.2(1), or a later release. The minimum DRAM memory requirements are as follows:
  - 32 MB, with one or two T1 lines
  - 48 MB, with three or four T1 lines
  - 64 MB, with five to ten T1 lines
  - 128 MB, with more than ten T1 lines

  The memory required for high-volume applications may be greater than that listed. Support for digital T1 packet voice trunk network modules is included in Plus feature sets. The IP Plus feature set requires 8 MB of Flash memory; other Plus feature sets require 16 MB.
- (Cisco 2600 and 3600 series routers) For digital E1 packet voice trunk network modules, install Cisco IOS Release 12.1(2)T, 12.2(1), or a later release. The minimum DRAM memory requirements are:
  - 48 MB, with one or two E1s
  - 64 MB, with three to eight E1s
  - 128 MB, with 9 to 12 E1s

  For high-volume applications, the memory required may be greater than these minimum values. Support for digital E1 packet voice trunk network modules is included in Plus feature sets. The IP Plus feature set requires 16 MB of Flash memory.
- (Cisco MC3810 concentrators) HCMs require Cisco IOS Release 12.0(7)XK or 12.1(2)T, 12.2(1), or a later release.
- (Cisco 7200 and 7500 series routers) For digital T1/E1 voice port adapters, install Cisco IOS Release 12.0(5)XE, 12.0(7)T, 12.2(1), or a later release. The minimum DRAM memory requirement to support T1/E1 high-capacity digital voice port adapters is 64 MB.

The memory required for high-volume applications may be greater than that listed. Support for T1/E1 high-capacity digital voice port adapters is included in Plus feature sets. The IP Plus feature set requires 16 MB of Flash memory.

7.356 ✓

Preparing Information to Configure Digital Voice Ports

Gather the following information about the telephony network connection that the voice port will be making:

- Line interface: T1 or E1
- Signaling interface: FXO, FXS, or E&M. If the interfaces are Primary Rate Interface (PRI) or BRI, see the "Configuring ISDN Interfaces for Voice" chapter in this configuration guide and *Cisco IOS Terminal Services Configuration Guide.*
- Line coding: AMI or B8ZS for T1, and AMI or HDB3 for E1
- Framing format: SF (D4) or ESF for T1, and CRC4 or no-CRC4 for E1
- Number of channels

Table 8 describes voice-port hardware configurations for various platforms. After the controllers have been configured, the **show voice port summary** command can also be used to determine available voice port numbers. If the **show voice port** command and a specific port number is entered, the default voice-port configuration for that port displays.

Table 8 Digital Voice Slot/Port Designations

Router Platform	Voice Hardware	Slot Number	Port Number
Cisco 2600 series	Digital T1/E1 Packet Voice Trunk Network Module (NM-HDV with VWIC-1MFT or VWIC-2MFT) One network module can be installed in a Cisco 2600 series router.	*slot* is the router location of the voice module. 1	*port* is the VWIC location in the network module. 0 to 1
Cisco 3600 series	Digital T1/E1 Packet Voice Trunk Network Module (NM-HDV with VWIC-1MFT or VWIC-2MFT) One network module can be installed in a Cisco 3620 router. A Cisco 3640 router can support three modules, and as many as six can be installed in a Cisco 3660 router.	*slot* is the router location of the voice module. 3620: 0 to 1 3640: 0 to 3 3660: 0 to 5	*port* is the VWIC location in the network module. 0 to 1

Table 8 Digital Voice Slot/Port Designations (continued)

Router Platform	Voice Hardware	Slot Number	Port Number
Cisco MC3810	• Digital voice module (DVM) • Voice compression module (VCM3 or VCM6) or • High-compression module (HCM2 or HCM6) VCM3 and VCM6 do not support codec complexity options.	1	—
Cisco AS5300	One Octal T1/E1 feature card (eight ports) or one Quad T1/E1 feature card (four ports) and one or two VFCs for voice and fax features.	—	*controller* is : Octal: 0 to 7 Quad: 0 to 3
Cisco AS5800	Up to four 12-port T1/E1 trunk cards and up to eight VFCs	*shelf* is 1 *slot* is 0 to 5	0 to 11
Cisco 7200 series	• Two-port T1/E1 enhanced digital voice port adapters • PA-VXC (high-capacity) • PA-VXB (moderate capacity) Port adapter slot 0 is reserved for the Fast Ethernet port on the I/O controller (if present).	Port adapter slot: from 1 to 4, or from 1 to 6	Interface port: 0 to 1
Cisco 7500 series	PA-VXB and PA-VXC on a VIP2 or VIP4 in Cisco 7500 series routers If the VIP is inserted in interface processor slot 3 and port adapter slot 0, then the addresses of the PA-VXB or PA-VXC are 3/0/0 or 3/0/1 (interface processor slot 3, port adapter slot 0, and interfaces 0 and 1).	Interface processor slot: 0 to 12 (depends on the number of slots in the router)	Port adapter slot: always 0 or 1 Interface port: 0 or 1

The following is **show voice port summary** sample output for a Cisco MC3810 multiservice concentrator:

7.354

```
Router# show voice port summary

IN      OUT
PORT    CH SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
====== == ========== ===== ==== ======== ======== ==
0:17    18 fxo-ls     down  down idle     on-hook  y
0:18    19 fxo-ls     up    dorm idle     on-hook  y
0:19    20 fxo-ls     up    dorm idle     on-hook  y
0:20    21 fxo-ls     up    dorm idle     on-hook  y
0:21    22 fxo-ls     up    dorm idle     on-hook  y
0:22    23 fxo-ls     up    dorm idle     on-hook  y
0:23    24 e&m-imd    up    dorm idle     idle     y
```

Platform-Specific Digital Voice Hardware

This section briefly describes digital voice hardware on the following platforms:

- Cisco 2600 series and Cisco 3600 series routers
- Cisco MC3810 multiservice concentrator
- Cisco AS5300 universal access server
- Cisco AS5800 universal access server
- Cisco 7200 series and Cisco 7500 series routers

Note For current information about supported hardware, see the release notes for the platform and Cisco IOS release you are using.

Cisco 2600 Series and Cisco 3600 Series Routers

Digital voice hardware on Cisco 2600 series and Cisco 3600 series modular access routers includes the high-density voice (HDV) network module and the multiflex trunk (MFT) voice/WAN interface card (VWIC). When an HDV is used in conjunction with an MFT and packet voice DSP modules (PVDMs), the HDV module is also called a *digital packet voice trunk network module*. The digital T1 or E1 packet voice trunk network module supports T1 or E1 applications, including fractional use. The T1 version integrates a fully managed data service unit/channel service unit (DSU/CSU), and the E1 version includes a fully managed DSU. The digital T1 or E1 packet voice trunk network module provides per-channel T1 or E1 data rates of 64 or 56 kbps for WAN services (Frame Relay or leased line).

Digital T1 or E1 packet voice trunk network modules for Cisco 2600 and 3600 series routers allow enterprises or service providers, using the voice-equipped routers as customer premise equipment (CPE), to deploy digital voice and fax relay. These network modules receive constant bit-rate telephony information over T1 or E1 interfaces and convert that information to a compressed format so that it can be sent over a packet network. The digital T1 or E1 packet voice trunk network modules can connect either to a PBX (or similar telephony device) or to a CO to provide PSTN connectivity. One digital T1 or E1 packet voice trunk network module can be installed in a Cisco 2600 series router or in a Cisco 3620 router. A Cisco 3640 router can support three network modules, and a Cisco 3660 router can support up to six network modules.

The MFT VWICs that are used in the packet voice trunk network modules are available in one- and two-port configurations for T1 and for E1, and in two-port configurations with drop-and-insert capability for T1 and E1. MFTs support the following kinds of traffic:

- Data. As WICs for T1 or E1 applications, including fractional data line use, the T1 version includes a fully managed DSU/CSU, and the E1 version includes a fully managed DSU.
- Packet voice. As VWICs included with the digital T1 or E1 packet voice trunk network module to provide connections to PBXs and COs, the MFTs enable packet voice applications.
- Multiplexed voice and data. Some two-port T1 or E1 VWICs can provide drop-and-insert multiplexing services with integrated DSU/CSUs. For example, when used with a digital T1 packet voice trunk network module, drop-and-insert allows 64-kbps DS0 channels to be taken from one T1 and digitally cross-connected to 64-kbps DS0 channels on another T1. Drop and insert, sometimes called TDM cross-connect, uses circuit switching rather than the DSPs that VoIP technology employs. (Drop-and-insert is described in the "Configuring Trunk Connections and Trunk Conditioning Features" chapter in this configuration guide.)

The digital T1 or E1 packet voice trunk network module contains five 72-pin Single In-line Memory Module (SIMM) sockets or banks, numbered 0 through 4, for PVDMs. Each socket can be filled with a single 72-pin PVDM, and there must be at least one packet voice data module (PVDM-12) in the network module to process voice calls. Each PVDM holds three digital signal processors (DSPs), so with five PVDM slots populated, a total of 15 DSPs are provided. High-complexity codecs support two simultaneous calls on each DSP, and medium-complexity codecs support four calls on each DSP. A digital T1 or E1 packet voice trunk network module can support the following numbers of channels:

- When the digital T1 or E1 packet voice trunk network module is configured for high-complexity codec mode, up to six voice or fax calls can be completed per PVDM-12, using the following codecs: G.711, G.726, G.729, G729 Annex A (E1), G.729 Annex B, G.723.1, G723.1 Annex A (T1), G.728, and fax relay.
- When the digital T1 or E1 packet voice trunk network module is configured for medium-complexity codec mode, up to 12 voice or fax calls can be completed per PVDM-12, using the following codecs: G.711, G.726, G.729 Annex A, G.729 Annex B with Annex A, and fax relay.

For more information, refer to the following publications:

- *Cisco 2600 Series Hardware Installation Guide*
- *Cisco 3600 Series Hardware Installation Guide*
- *Cisco Network Module Hardware Installation Guide*
- Cisco IOS Release 12.0(7)T online document *Configuring 1- and 2-Port T1/E1 Multiflex Voice/WAN Interface Cards on Cisco 2600 and 3600 Series Routers*

Cisco MC3810 Multiservice Concentrator

To support a T1 or E1 digital voice interface, the Cisco MC3810 multiservice concentrator must be equipped with a digital voice interface card (DVM). The DVM interfaces with a digital PBX, channel bank, or video codec. It supports up to 24 channels of compressed digital voice at 8 kbps, or it can cross-connect channelized data from user equipment directly onto the router's trunk port for connection to a carrier network.

The DVM is available with a balanced interface using an RJ-48 connector or with an unbalanced interface using Bayonet-Neill-Concelman (BNC) connectors.

Optional HCMs can replace standard VCMs to operate according to the voice compression coding algorithm (codec) specified when the Cisco MC3810 multiservice concentrator is configured. The HCM2 provides 4 voice channels at high codec complexity and 8 channels at medium complexity. The

HCM6 provides 12 voice channels at high complexity and 24 channels at medium complexity. You can install one or two HCMs in a Cisco MC3810, but an HCM can not be combined with a VCM in the same chassis.

For more information, refer to the following publications:

- *Cisco MC3810 Multiservice Concentrator Hardware Installation Guide*
- *Overview of the Cisco MC3810 Series*
- *Configuring Cisco MC3810 Series Concentrators to Use High-Performance Compression Modules*

Cisco AS5300 Universal Access Server

The Cisco AS5300 Universal Access Server includes three expansion slots. One slot is for either an Octal T1/E1/PRI feature card (eight ports) or a Quad T1/E1/PRI feature card (four ports), and the other two can be used for voice/fax or modem feature cards. Because a single voice/fax feature card (VFC) can support up to 48 (T1) or 60 (E1) voice calls, the Cisco AS5300/Voice Gateway system can support a total of 96 or 120 simultaneous voice calls. The use of VFCs requires Cisco IOS release 12.0.2XH or later.

Cisco AS5300 VFCs are coprocessor cards, each with a powerful reduced instruction set computing (RISC) engine and dedicated, high-performance DSPs to ensure predictable, real-time voice processing. The design couples this coprocessor with direct access to the Cisco AS5300 routing engine for streamlined packet forwarding.

For more information, refer to the following publications:

- *Cisco AS5300 Chassis Installation Guide*
- *Cisco AS5300 Module Installation Guide*

Cisco AS5800 Universal Access Server

The Cisco AS5800 Universal Access Server consists of two primary system components: the Cisco 5814 dial shelf (DS), which holds channelized trunk cards and connects to the PSTN, and the Cisco 7206 router shelf (RS), which holds port adapters and connects to the IP backbone.

The dial shelf acts as the access concentrator by accepting and consolidating all types of remote traffic, including voice, dial-in analog and digital ISDN data, and industry-standard WAN and remote connection types. The dial shelf also contains controller cards voice feature cards, modem feature cards, trunk cards, and dial shelf interconnect cards.

One or two dial shelf controllers (DSCs) provide clock and power control to the dial shelf cards. Each DSC contains a block of logic that is referred to as the common logic and system clocks. This block of logic can use a variety of sources to generate the system timing, including an E1 or T1/T3 input signal from the BNC connector on the DSC's front panel. The configuration commands for the master clock specify the various clock sources and a priority for each source (see the "Clock Sources on Digital T1/E1 Voice Ports" section on page 68).

The Cisco AS5800 voice feature card is a multi-DSP coprocessing board and software package that adds VoIP capabilities to the Cisco AS5800 platform. The Cisco AS5800 voice feature card, when used with other cards such as LAN/WAN and modem cards, provides a gateway for up to 192 packetized voice/fax calls and 360 data calls per card. A Cisco AS5800 can support up to 1,344 voice calls in split-dial-shelf configuration with two 7206VXR router shelves.

For more information, refer to the following publications:

- *Cisco AS5800 Universal Access Server Operation, Administration, Maintenance, and Provisioning Guide*
- *Cisco AS5800 Access Server Hardware Installation Guide*

Cisco 7200 and Cisco 7500 Series Routers

Cisco 7200 and Cisco 7500 series routers support multimedia routing and bridging with a wide variety of protocols and media types. The Cisco 7000 family versatile interface processor (VIP) is based on a RISC engine optimized for I/O functions. To this engine are attached one or two port adapters or daughter boards, which provide the media-specific interfaces to the network. The network interfaces provide connections between the routers' peripheral component interconnect (PCI) buses and external networks. Port adapters can be placed in any available port adapter slot, in any desired combination.

T1/E1 high-capacity digital voice port adapters for Cisco 7200 and Cisco 7500 series routers allow enterprises or service providers, using the equipped routers as customer premise equipment, to deploy digital voice and fax relay. These port adapters receive constant bit-rate telephony information over T1/E1 interfaces and can convert that information to a compressed format for transmission as voice over IP (VoIP). Two types of digital voice port adapters are supported on Cisco 7200 and Cisco 7500 series routers: two-port high-capacity (up to 48 or 120 channels of compressed voice, depending on codec choice), and two-port moderate capacity (up to 24 or 48 channels of compressed voice). These single-width port adapters incorporate two universal ports configurable for either T1 or E1 connection, for use with high-performance digital signal processors (DSPs). Integrated CSU/DSUs, echo cancellation, and DS0 drop-and-insert functionality eliminate the need for external line termination devices and multiplexers.

For more information, refer to the following publications:

- *Cisco 7200 VXR Installation and Configuration Guide*
- *Cisco 7500 Series Installation and Configuration Guide*
- *Two-Port T1/E1 Moderate-Capacity and High-Capacity Digital Voice Port Adapter Installation and Configuration*

Note For current information about supported hardware, see the release notes for the platform and Cisco IOS release being used.

Configuring Basic Parameters on Digital T1/E1 Voice Ports

This section describes commands for basic digital voice port configuration. Make sure you have all the data recommended in the "Preparing Information to Configure Digital Voice Ports" section on page 58 before starting this procedure.

4.350

The basic steps for configuring digital voice ports are described in the next three sections. They are grouped by the configuration mode from which they are executed, as follows:

- Configuring Codec Complexity for Digital T1/E1 Voice Ports, page 64

  Codec complexity refers to the amount of processing power assigned to codec processing on a voice port. On most router platforms that support codec complexity, codec complexity is selected in voice card configuration mode, although it is selected in DSP interface mode on the Cisco 7200 and 7500 series. The value configured for codec complexity establishes the choice of codecs that are available on the dial peers. See the *Configuring Dial Plans, Dial Peers, and Digit Manipulation* chapter in this configuration guide for more information about configuring dial peers.
- Configuring Controller Settings for Digital T1/E1 Voice Ports, page 67

  Specific line characteristics must be configured to match those of the PSTN line that is being connected to the voice port. These are typically configured in controller configuration mode.
- Configuring Basic Voice Port Parameters for Digital T1/E1 Voice Ports, page 78

  Voice port configuration mode allows many of the basic voice call attributes to be configured to match those of the PSTN or PBX connection being made on this voice port.

In addition to the basic voice port parameters, there are additional commands that allow for the fine-tuning of the voice port configurations or for configuration of optional features. In most cases, the default values for these commands are sufficient for establishing voice port configurations. If it is necessary to change some of these parameters to improve voice quality or to match parameters in proprietary PBXs to which you are connecting, use the commands in the "Fine-Tuning Analog and Digital Voice Ports" section on page 80.

After voice port configuration, make sure the ports are operational by following the steps described in these sections:

- Verifying Analog and Digital Voice-Port Configurations, page 99
- Troubleshooting Analog and Digital Voice Port Configurations, page 110

For more information on voice port commands, refer to the *Cisco IOS Voice, Video, and Fax Command Reference*.

Configuring Codec Complexity for Digital T1/E1 Voice Ports

On the Cisco 2600, 3600, 7200, and 7500 routers, codec complexity can be configured separately for each T1/E1 digital packet voice trunk network module or port adapter. On a Cisco MC3810 multiservice concentrator, only a single codec complexity setting is used, even when two HCMs are installed. The value specified in this task affects the choice of codecs available when the **codec** dial-peer configuration command is configured.

For details on the number of calls that can be handled simultaneously using each of the codec standards, refer to the entries for **codec** and **codec complexity** in the *Cisco IOS Voice, Video, and Fax Command Reference* and to platform-specific product literature.

For more information on codec complexity, see the "Configuring Codec Complexity for Analog Voice Ports on the Cisco MC3810 with High-Performance Compression Modules" section on page 47.

Two configuration task tables are shown below: one for the Cisco 2600 and 3600 series routers and the Cisco MC3810 concentrator, which use voice card configuration mode, and the second for the Cisco 7200 and 7500 series routers, which use DSP interface configuration mode.

Cisco 2600 and 3600 Series and Cisco MC3810

This procedure applies to voice ports on digital packet voice trunk network modules on Cisco 2600 series and Cisco 3600 series routers, and to voice ports on HCMs on Cisco MC3810 multiservice concentrators.

Note On Cisco 2600 and 3600 series routers with digital T1/E1 packet voice trunk network modules, codec complexity cannot be configured if DS0 groups are configured. Use the **no ds0-group** command to remove DS0 groups before configuring codec complexity.

Note On the Cisco MC3810 multiservice concentrator with high compression modules, check the DSP voice channel activity with the **show voice dsp** command. If any DSP voice channels are in the busy state, you cannot change the codec complexity. When all of the DSP channels are in the idle state, you can make changes to the codec complexity selection.

To configure codec complexity, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router# show voice dsp`	Checks the DSP voice channel activity. If any DSP voice channels are in the busy state, codec complexity cannot be changed. When all of the DSP channels are in the idle state, continue to Step 2.
Step 2	`Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# voice-card slot`	Enters voice card configuration mode for the card or cards in the slot specified. For the Cisco 2600 and 3600 series routers, the *slot* argument ranges from 0 to 5. For the Cisco MC3810 multiservice concentrator, *slot* must be 0.
Step 4	`Router(config-voicecard)# codec complexity {high | med}`	Specifies codec complexity based on the codec standard being used. This setting restricts the codecs available in dial peer configuration. All voice cards in a router must use the same codec complexity setting. The keywords are as follows: • **high**—(Optional) Specifies up to six voice or fax calls completed per PVDM-12, using the following codecs: G.711, G.726, G.729, G.729 Annex B, G.723.1, G.723.1 Annex A, G.728, and fax relay. • **med**—(Optional) Supports up to 12 voice or fax calls completed per PVDM-12, using the following codecs: G.711, G.726, G.729 Annex A, G.729 Annex B with Annex A, and fax relay. The default is **med**. **Note** On the Cisco MC3810 multiservice concentrator, this command is valid only with one or more HCMs installed, and voice card 0 must be specified. If two HCMs are installed, this command configures both HCMs at once.

7.348

Cisco AS5300 Universal Access Server

Codec support on the Cisco AS5300 universal access server is determined by the capability list on the voice feature card, which defines the set of codecs that can be negotiated for a voice call. The capability list is created and populated when VCWare is unbundled and DSPWare is added to VFC Flash memory. The capability list does not indicate codec preference; it simply reports the codecs that are available. The session application decides which codec to use. Codec support is configured on dial peers rather than on voice ports; see the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter in this configuration guide.

Cisco AS5800 Universal Access Server

Selection of codec support on Cisco AS5800 access servers is made during dial peer configuration. See the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter in this configuration guide.

Cisco 7200 Series and Cisco 7500 Series Routers

On Cisco 7200 series and Cisco 7500 series routers, codec complexity is configured on the DSP interface.

Note Check the DSP voice channel activity using the **show interfaces dspfarm** command. If any DSP voice channels are in the busy state, codec complexity cannot be changed. When all of the DSP channels are in the idle state, changes can be made to the codec complexity selection.

To configure the DSP interface, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	`Router#` **`show interfaces dspfarm`**	Displays the DSP voice channel activity. If any DSP voice channels are in the busy state, codec complexity cannot be changed. When all of the DSP channels are in the idle state, continue to Step 2.
Step 2	`Router#` **`configure terminal`**	Enters global configuration mode.

Step 3	**Cisco 7200 series**
	`Router(config)#` **`dspint dspfarm`** *`slot/port`*
	Cisco 7500 series
	`Router(config)#` **`dspint dspfarm`** *`slot/port-adapter/port`*
		Enters DSP interface configuration mode. The arguments are as follows:
		• *slot/port*—Specifies the slot and port numbers of the interface.
		• *adapter/port*—Specifies the adapter and port numbers of the interface.

	Command	Purpose
Step 4	`Router(config-dspfarm)# codec {high | med}`	Specifies the codec complexity based on the codec standard being used. The keyword specified for **codec** affects the choice of codecs available when the **codec** dial-peer configuration command is used. The keywords are as follows: • **high**—Supports two voice channels encoded in any of the following formats: G.711, G.726, G.729, G.729 Annex B, G.723.1, G.723.1 Annex A, G.728, and fax relay. • **med**—(default) Supports up to four calls using the following codecs: G.711, G.726, G.729 Annex A, G.729 Annex B with Annex A, and fax relay.
Step 5	`Router(config-dspfarm)# description`	Enters a string to include descriptive text about this DSP interface connection. This information is displayed in the output for **show** commands and does not affect the operation of the interface in any way.

Configuring Controller Settings for Digital T1/E1 Voice Ports

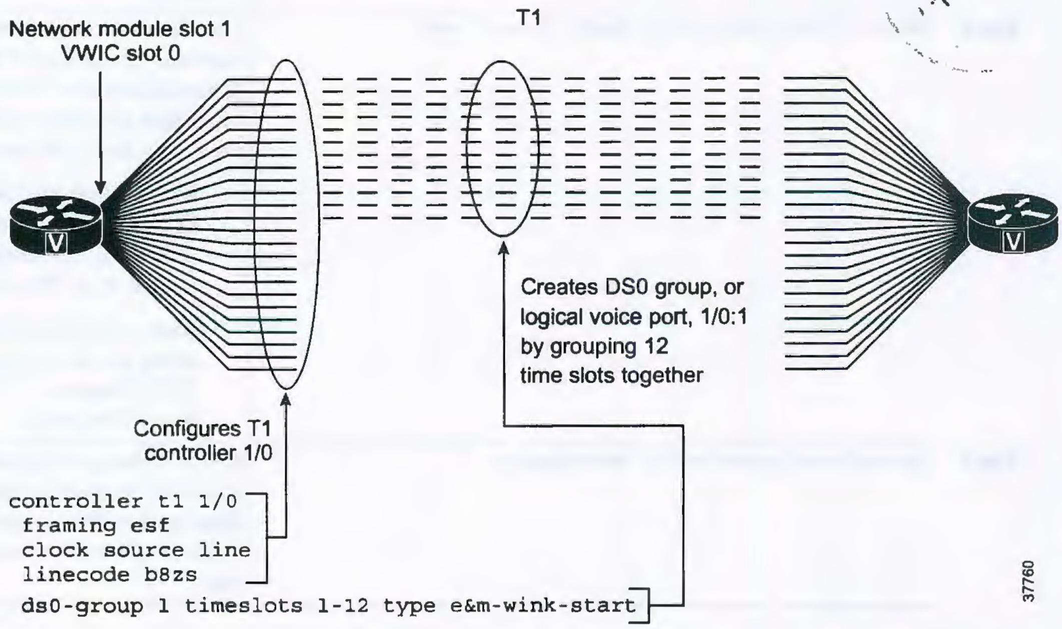
The purpose of configuring controllers for digital T1/E1 voice ports is to match the configuration of the router to the line characteristics of the telephony network connection being made so that voice and signaling can be transferred between them and so that logical voice ports, or DS0 groups, may be established.

Figure 16 shows how a **ds0-group** command gathers some of the DS0 time slots from a T1 line into a group that becomes a single logical voice port, which can later be addressed as a single entity in voice port configurations. Other DS0 groups for voice can be created from the remaining time slots shown in the figure, or the time slots can be used for data or serial pass-through.

Note that all the controller commands in Figure 16 other than **ds0-group** apply to all the time slots in the T1.

7.346

Figure 16 T1 Controller Configuration on Cisco 2600 or 3600 Series Routers



```
controller t1 1/0
 framing esf
 clock source line
 linecode b8zs
 ds0-group 1 timeslots 1-12 type e&m-wink-start
```

Voice port controller configuration includes setting the parameters described in the following sections:

- Framing Formats on Digital T1/E1 Voice Ports
- Clock Sources on Digital T1/E1 Voice Ports
- Line Coding on Digital T1/E1 Voice Ports
- DS0 Groups on Digital T1/E1 Voice Ports

Another controller command that might be needed, **cablelength**, is discussed in the *Cisco IOS Interface Command Reference*, Release 12.2.

Framing Formats on Digital T1/E1 Voice Ports

The framing format parameter describes the way that bits are robbed from specific frames to be used for signaling purposes. The controller must be configured to use the same framing format as the line from the PBX or CO that connects to the voice port you are configuring.

Digital T1 lines use super frame (SF) or extended super frame (ESF) framing formats. SF provides two-state, continuous supervision signaling, in which bit values of 0 are used to represent on-hook and bit values of 1 are used to represent off-hook. ESF robs four bits instead of two, yet has little impact on voice quality. ESF is required for 64-kbps operation on DS0 and is recommended for Primary Rate Interface (PRI) configurations.

E1 lines can be configured for cyclic redundancy check (CRC4) or no cyclic redundancy check, with an optional argument for E1 lines in Australia.

Clock Sources on Digital T1/E1 Voice Ports

Digital T1/E1 interfaces use timers called *clocks* to ensure that voice packets are delivered and assembled properly. All interfaces handling the same packets must be configured to use the same source of timing so that packets are not lost or delivered late. The timing source that is configured can be external (from the line) or internal to the router's digital interface.

7.345

If the timing source is internal, timing derives from the onboard phase-lock loop (PLL) chip in the digital voice interface. If the timing source is line (external), then timing derives from the PBX or PSTN CO to which the voice port is connected. It is generally preferable to derive timing from the PSTN because their clocks are maintained at an extremely accurate level. This is the default setting for the clocks. When two or more controllers are configured, one should be designated as the primary clock source; it will drive the other controllers.

The **line** keyword specifies that the clock source is derived from the active line rather than from the free-running internal clock. The following rules apply to clock sourcing on the controller ports:

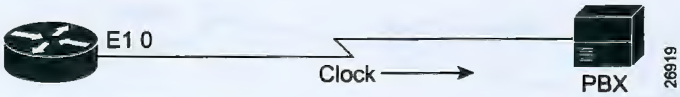
- When both ports are set to line clocking with no primary specification, port 0 is the default primary clock source and port 1 is the default secondary clock source.
- When both ports are set to line and one port is set as the primary clock source, the other port is by default the backup or secondary source and is loop-timed.
- If one port is set to clock source line or clock source line primary and the other is set to clock source internal, the internal port recovers clock from the clock source line port if the clock source line port is up. If it is down, then the internal port generates its own clock.
- If both ports are set to clock source internal, there is only one clock source: internal.

This section describes the five basic timing scenarios that can occur when a digital voice port is connected to a PBX or CO. In all the examples that follow, the PSTN (or CO) and the PBX are interchangeable for purposes of providing or receiving clocking.

- Single Voice Port Providing Clocking—In this scenario, the digital voice hardware is the clock source for the connected device, as shown in Figure 17. The PLL generates the clock internally and drives the clocking on the line. Generally, this method is useful only when connecting to a PBX, key system, or channel bank. A Cisco VoIP gateway rarely provides clocking *to* the CO because CO clocking is much more reliable. The following configuration sets up this clocking method for a digital E1 voice port:

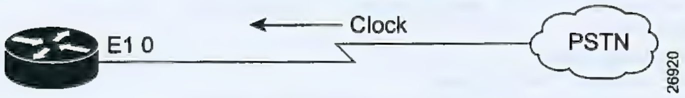
```
controller E1 1/0
 framing crc4
 linecoding hdb3
 clock source internal
 ds0-group timeslots 1-15 type e&m-wink-start
```

Figure 17 Single Voice Port Providing Clocking



- Single Voice Port Receiving Internal Clocking—In this scenario, the digital voice hardware receives clocking from the connected device (CO telephony switch or PBX) (see Figure 18). The PLL clocking is driven by the clock reference on the receive (Rx) side of the digital line connection.

Figure 18 Single E1 Port Receiving Clocking from the Line



7.344

The following configuration sets up this clocking method:

```
controller T1 1/0
 framing esf
 linecoding ami
 clock source line
 ds0-group timeslots 1-12 type e&m-wink-start
```

- Dual Voice Ports Receiving Clocking from the Line—In this scenario, the digital voice port has two reference clocks, one from the PBX and another from the CO, as shown in Figure 19. Because the PLL can derive clocking from only one source, this case is more complex than the two preceding examples.

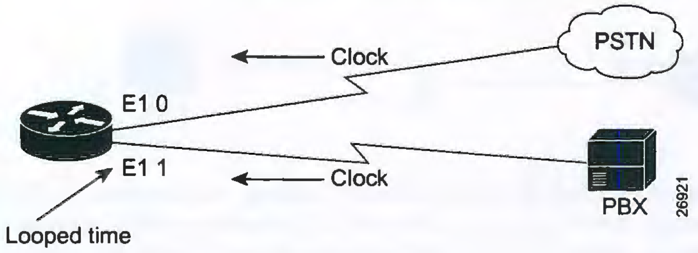
  Before looking at the details, consider the following as they pertain to the clocking method:

  - Looped-time clocking: The voice port takes the clock received on its Rx (receive) pair and regenerates it on its Tx (transmit) pair. While the port receives clocking, the port is not driving the PLL on the card but is "spoofing" (that is, fooling) the port so that the connected device has a viable clock and does not see slips (that is, loss of data bits). PBXs are not designed to accept slips on a T1 or E1 line, and such slips cause a PBX to drop the link into failure mode. While in looped-time mode, the router often sees slips, but because these are controlled slips, they usually do not force failures of the router's voice port.
  - Slips: These messages indicate that the voice port is receiving clock information that is out of phase (out of synchronization). Because the router has only a single PLL, it can experience controlled slips while it receives clocking from two different time sources. The router can usually handle controlled slips because its single-PLL architecture anticipates them.

Note Physical layer issues, such as bad cabling or faulty clocking references, can cause slips. Eliminate these slips by addressing the physical layer or clock reference problems.

In the dual voice ports receiving clocking from the line scenario, the PLL derives clocking from the CO and puts the voice port connected to the PBX into looped-time mode. This is usually the best method because the CO provides an excellent clock source (and the PLL usually requires that the CO provide that source) and a PBX usually must receive clocking from the other voice port.

Figure 19 Dual E1 Ports Receiving Clocking from the Line



The following configuration sets up this clocking method:

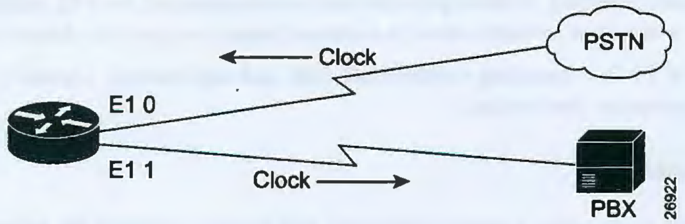
```
controller E1 1/0 << description - connected to the CO
 framing crc4
 linecoding hdb3
 clock source line primary
 ds0-group timeslots 1-15 type e&m-wink-start
!
```

```
controller E1 1/1 << description - connected to the PBX
 framing crc4
 linecoding hdb3
 clock source line
 ds0-group timeslots 1-15 type e&m-wink-start
```

The **clock source line primary** command tells the router to use this voice port to drive the PLL. All other voice ports configured as **clock source line** are then put into an implicit loop-timed mode. If the primary voice port fails or goes down, the other voice port instead receives the clock that drives the PLL. In this configuration, port 1/1 might see controlled slips, but these should not force it down. This method prevents the PBX from seeing slips.

- Dual Voice Ports (One Receives Clocking and One Provides Clocking)—In this scenario, the digital voice hardware receives clocking for the PLL from E1 0 and uses this clock as a reference to clock E1 1 (see Figure 20). If controller E1 0 fails, the PLL internally generates the clock reference to drive E1 1.

Figure 20 Dual E1 ports—One Receiving and One Providing Clocking

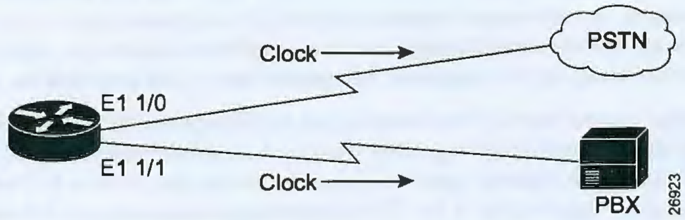


The following configuration sets up this clocking method:

```
controller E1 1/0
 framing crc4
 linecoding hdb3
 clock source line
 ds0-group timeslots 1-15 type e&m-wink-start
!
controller E1 1/1
 framing crc4
 linecoding hdb3
 clock source internal
 ds0-group timeslots 1-15 type e&m-wink-start
```

- Dual Voice Ports (Router Provides Both Clocks)—In this scenario, the router generates the clock for the PLL and, therefore, for both voice ports (see Figure 21).

Figure 21 Dual E1 Ports—both Clocks from the Router



The following configuration sets up this clocking method:

```
controller E1 1/0
 framing crc4
 linecoding hdb3
 clock source internal
 ds0-group timeslots 1-15 type e&m-wink-start
!
controller E1 1/1
 framing esf
 linecoding b8zs
 clock source internal
 ds0-group timeslots 1-15 type e&m-wink-start
```

Line Coding on Digital T1/E1 Voice Ports

Digital T1/E1 interfaces require that line encoding be configured to match that of the PBX or CO that is being connected to the voice port. Line encoding defines the type of framing used on the line.

T1 line encoding methods include alternate mark inversion (AMI) and binary 8 zero substitution (B8ZS). AMI is used on older T1 circuits and references signal transitions with a binary 1, or "mark." B8ZS, a more reliable method, is more popular and is recommended for PRI configurations as well. B8ZS encodes a sequence of eight zeros in a unique binary sequence to detect line-coding violations.

Supported E1 line encoding methods are AMI and high-density bipolar 3 (HDB3), which is a form of zero-suppression line coding.

DS0 Groups on Digital T1/E1 Voice Ports

For digital voice ports, a single command, **ds0-group**, performs the following functions:

- Defines the T1/E1 channels for compressed voice calls.
- Automatically creates a logical voice port.

  The numbering for the logical voice port created as a result of this command is *controller:ds0-group-no*, where *controller* is defined as the platform-specific address for a particular controller. On a Cisco 3640 router, for example, **ds0-group 1 timeslots 1-24 type e&m-wink** automatically creates the voice port 1/0:1 when issued in the configuration mode for controller 1/0. On a Cisco MC3810 universal concentrator, when you are in the configuration mode for controller 0, the command **ds0-group 1 timeslots 1-24 type e&m-wink** creates logical voice port 0:1.

  To map individual DS0s, define additional DS0 groups under the T1/E1 controller, specifying different time slots. Defining additional DS0 groups also creates individual DS0 voice ports.

- Defines the emulated analog signaling method that the router uses to connect to the PBX or PSTN

  Most digital T1/E1 connections used for switch-to-switch (or switch-to-router) trunks are E&M connections, but FXS and FXO connections are also supported. These are normally used to provide emulated-OPX (Off-Premises eXtension) from a PBX to remote stations. FXO ports connect to FXS ports. The FXO or FXS connection between the router and switch (CO or PBX) must use matching signaling, or calls cannot connect properly. Either ground start or loop start signaling is appropriate for these connections. Ground start provides better disconnect supervision to detect when a remote user has hung up the telephone, but ground start is not available on all PBXs.

  Digital ground start differs from digital E&M because the A and B bits do not track each other as they do in digital E&M signaling (that is, A is not necessarily equal to B). When the CO delivers a call, it *seizes* a channel (goes off-hook) by setting the A bit to 0. The CO equipment also simulates ringing by toggling the B bit. The terminating equipment goes off-hook when it is ready to answer the call. Digits are usually not delivered for incoming calls.

E&M connections can use one of three different signaling types to acknowledge on-hook and off-hook states: wink start, immediate start, and delay start. E&M wink start is usually preferred, but not all COs and PBXs can handle wink start signaling. The E&M connection between the router and switch (CO or PBX) must match the CO or PBX E&M signaling type, or calls cannot be connected properly.

E&M signaling is normally used for trunks. It is normally the only way that a CO switch can provide two-way dialing with Direct Inward Dialing (DID). In all the E&M protocols, off-hook is indicated by A=B=1 and on-hook is indicated by A=B=0 (robbed-bit signaling). If dial pulse dialing is used, the A and B bits are pulsed to indicate the addressing digits. The are several further important subclasses of E&M robbed-bit signaling:

- E&M Wink Start—Feature Group B

  In the original wink start handshaking protocol, the terminating side responds to an off-hook from the originating side with a short wink (transition from on-hook to off-hook and back again). This wink tells the originating side that the terminating side is ready to receive addressing digits. After receiving addressing digits, the terminating side then goes off-hook for the duration of the call. The originating endpoint maintains off-hook for the duration of the call.

- E&M Wink Start—Feature Group D

  In Feature Group D wink start with wink acknowledge handshaking protocol, the terminating side responds to an off-hook from the originating side with a short wink (transition from on-hook to off-hook and back again) just as in the original wink start. This wink tells the originating side that the terminating side is ready to receive addressing digits. After receiving addressing digits, the terminating side provides another wink (called an *acknowledgment wink*) that tells the originating side that the terminating side has received the dialed digits. The terminating side then goes off-hook to indicate connection. This last indication can be due to the ultimate called endpoint's having answered. The originating endpoint maintains an off-hook condition for the duration of the call.

- E&M Immediate Start

  In the immediate-start protocol, the originating side does not wait for a wink before sending addressing information. After receiving addressing digits, the terminating side then goes off-hook for the duration of the call. The originating endpoint maintains off-hook for the duration of the call.

Note Feature Group D is supported on Cisco AS5300 platforms, and on Cisco 2600, 3600, and 7200 series with digital T1 packet voice trunk network modules. Feature Group D is not supported on E1 or analog voice ports.

7.340

To configure controller settings for digital T1/E1 voice ports, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	**Cisco 7200 and 7500 series** `Router(config)# card type {t1 | e1} slot`	Defines the card as T1 or E1 and stipulates the location. The keywords and arguments are as follows: • **t1** | **e1**—Defines the type of card. • *slot*—A value from 0 to 5.

Step 2	**Cisco 2600 and 3600 series, Cisco MC3810, and Cisco 7200 series**
	`Router(config)# controller {t1 | e1} slot/port`
	Cisco AS5300
	`Router(config)# controller {t1 | e1} number`
	Cisco AS5800
	`Router(config)# controller {t1 | e1} shelf/slot/port`
	Cisco 7500 series
	`Router(config)# controller {t1 | e1} slot/port-adapter/slot`
		Enters controller configuration mode.
		The keywords and arguments are as follows:
		• **t1** | **e1**—The type of controller.
		• *slot/port*—The backplane slot number and port number for the interface being configured.
		• *number*—The network processor module number; the range is from 0 to 2.
		• *shelf/slot/port*—Indicates the controller ports; the range for *port* is from 0 to 11.

Step 3	**T1**
	`Router(config-controller)# framing {sf | esf}`
	E1
	`Router(config-controller)# framing {crc4 | no-crc4} [australia]`
		Selects frame type for T1 or E1 line.
		The keywords and arguments are as follows:
		T1 lines
		• **sf**—super frame
		• **esf**—extended super frame
		E1 lines
		• **crc4**—Provides 4 bits of error protection.
		• **no-crc4**—Disables **crc4**.
		• **australia**—(Optional) Specifies the E1 frame type used in Australia.
		The default for T1 is **sf**.
		The default for E1 is **crc4**.

7.339

	Command	Purpose
Step 4	Router(config-controller)# **clock source** {**line** [**primary** | **secondary**] | **internal**}	Configures the clock source. The keywords and arguments are as follows: • **line**—Specifies that the PLL on this port derives clocking from the external source to which the port is connected (generally the CO). • **primary**—(Optional) Specifies that the PLL on this port derives clocking from the external source and puts the other port (generally connected to the PBX) into looped-time mode. Both ports are configured with **line**, but only the port connected to the external source is configured with **primary**. • **secondary**—(Optional) Indicates a backup external source for clocking if the primary clocking shuts down. Configure the **clock source line secondary** command on the controller that has the next-best-known clocking. • **internal**—(Optional) Specifies that the clock is generated from the voice port's internal PLL. For more information about clock sources, see the "Clock Sources on Digital T1/E1 Voice Ports" section on page 68. The default is **line**.

Step 5	**T1 lines**
	Router(config-controller)# **linecode** {**ami** | **b8zs**}
	E1 lines
	Router(config-controller)# **linecode** {**ami** | **hdb3**}
		Specifies the line encoding to use.
		The keywords are as follows:
		• **ami**—Specifies the alternate mark inversion (AMI) line code type. (T1 and E1)
		• **b8zs**—Specifies the binary 8 zero substitution (B8ZS) line code type. (T1 only)
		• **hdb3**—Specifies the high-density bipolar 3 (HDB3) line code type. (E1 only)
		The default for T1 is **ami**.
		The default for E1 is **hdb3**.

7.338 >

	Command	Purpose
Step 6	**Cisco 2600 and 3600 Series Routers and Cisco MC3810 Multiservice Concentrators—T1** Router(config-controller)# **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-fgd** | **e&m-immediate-start** **e&m-wink-start** | **ext-sig** | **fgd-eana** | **fxo-ground-start** | **fxo-loop-start** | **fxs-ground-start** | **fxs-loop-start**} **Cisco 2600 and 3600 Series Routers and Cisco MC3810 Multservice Concentrators—E1** Router(config-controller)# **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** {**e&m-delay-dial** | **e&m-immediate-start** | **e&m-melcas-delay** | **e&m-melcas-immed** | **e&m-melcas-wink** | **e&m-wink-start** | **ext-sig** | **fgd-eana** | **fxo-ground-start** | **fxo-loop-start** | **fxo-melcas** | **fxs-ground-start** | **fxs-loop-start** | **fxs-melcas** | **r2-analog** | **r2-digital** | **r2-pulse**} **Cisco AS5300 Universal Access Servers—T1** Router(config-controller)# **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* [**service** {**data** | **fax** | **voice**}] [**type** {**e&m-fgb** | **e&m-fgd** | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** | **fgd-os** | **r1-itu** | **sas-ground-start** | **sas-loop-start** | **none**}] **Cisco AS5300 Universal Access Servers—E1** Router(config-controller)# **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** {**none** | **p7** | **r2-analog** | **r2-digital** | **r2-lsv181-digital** | **r2-pulse**} **Cisco AS5800 Universal Access Servers—T1** Router(config-controller)# **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** {**e&m-fgb** | **e&m-fgd** | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **fgd-eana** | **r1-itu** | **r1-modified** | **r1-turkey** | **sas-ground-start** | **sas-loop-start** | **none**} **Cisco AS5800 Universal Access Servers E1 Voice Ports** Router(config-controller)# **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** {**e&m-fgb** | **e&m-fgd** | **e&m-immediate-start** | **fxs-ground-start** | **fxs-loop-start** | **p7** | **r2-analog** | **r2-digital** | **r2-pulse** | **sas-ground-start** | **sas-loop-start** | **none**} **Cisco 7200 and 7500 Series Series Routers T1 and E1 Voice Ports** Router(config-controller)# **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** {**e&m-delay** | **e&m-immediate** | **e&m-wink** | **fxs-ground-start** | **fxs-loop-start** | **fxo-ground-start** | **fxo-loop-start**}	Defines the T1 channels for use by compressed voice calls and the signaling method that the router uses to connect to the PBX or CO. **Note** This step shows the basic syntax and signaling types available with the **ds0-group** command. For the complete syntax, see the *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2. The keywords and arguments are as follows: • *ds0-group-no*—Identifies the DS0 group (number from 0 to 23, for T1, or from 0 to 30, for E1). • **timeslots** *timeslot-list*—Specifies the single time slot number, single range of numbers, or multiple ranges of numbers separated by commas. For T1/E1, allowable values are from 1 to 24. Examples are as follows: – 2, 3-5 – 1, 7, 9 – 1-12 • **service**—Indicates the type of calls to be handled by this DS0 group—data, fax, or voice). • **type**—Refers to the signaling type of the telephony connection being made. Types include the following: – **e&m-delay-dial**—Specifies the originating endpoint that sends an off-hook signal and waits for the off-hook signal followed by an on-hook signal from the destination. – **e&m-fgb**—E & M Type II Feature Group B. – **e&m-fgd**—E & M Type II Feature Group D.

7.337
J

	Command	Purpose
		- **e&m-immediate-start**—E & M Immediate Start. - **e&m-melcas-delay**—E&M Mercury Exchange Limited Channel Associated Signaling (MELCAS) delay start signaling support. - **e&m-melcas-immed**—E&M MELCAS immediate start signaling support. - **e&m-melcas-wink**—E&M MELCAS wink start signaling support. - **e&m-wink-start**—The originating endpoint sends an off-hook signal and waits for a - **ext-sig**—For the specified channel, automatically generates the off-hook signal and stays in the off-hook state. - **fgd-eana**—Feature Group D Exchange Access North American. - **fgd-os**—Feature Group D Operator Services. - **fxo-melcas**—MELCAS Foreign Exchange Office signaling support. - **fxs-melcas**—MELCAS Foreign Exchange Station signaling support. - **fxs-ground-start**—FXS Ground Start. - **fxs-loop-start**—FXS Loop Start. - **none**—Null Signaling for External Call Control. - **p7**—Specifies the p7 switch type. - **r1-itu**—R1 ITU - **sas-ground-start**—SAS Ground Start. - **sas-loop-start**—SAS Loop Start. The **r1** and **r2** keywords refer to line signaling, based on international signaling standards. The **r1 itu** keywords are based on signaling standards in countries besides the United States. An "ITU variant" means that there are multiple R1 standards in a particular country but that Cisco supports the ITU variant.
Step 7	`Router(config-controller)# no shutdown`	Activates the controller.

7.336

Configuring Basic Voice Port Parameters for Digital T1/E1 Voice Ports

For FXO and FXS connections the default voice-port parameter values are often adequate. However, for E&M connections, it is important to match the characteristics of your PBX, so voice port parameters may need to be reconfigured from their defaults.

Each voice port that you address in digital voice port configuration is one of the logical voice ports that you created with the **ds0-group** command.

Companding (from *compression* and *expansion*), used in Step 4 of the following table, is the part of the PCM process in which analog signal values are logically rounded to discrete scale-step values on a nonlinear scale. The decimal step number is then coded in its binary equivalent prior to transmission. The process is reversed at the receiving terminal using the same nonlinear scale.

Note The commands, keywords, and arguments that you are able to use may differ slightly from those presented here, based on your platform, Cisco IOS release, and configuration. When in doubt, use Cisco IOS command help (**command ?**) to determine the syntax choices that are available.

To configure basic parameters for digital T1/E1 voice ports, use the following commands beginning in global configuration mode.

	Command	Purpose

Step 1	**Cisco 2600 and 3600 Series Routers**
	`Router(config)# voice-port slot/port:ds0-group-no`
	Cisco MC3810 Multiseries Concentrators
	`Router(config)# voice-port slot:ds0-group-no`
	Cisco AS5300 Universal Access Server
	`Router(config)# voice-port controller:ds0-group-no`
	Cisco AS5800 Universal Access Server
	`Router(config)# voice-port shelf/slot/port:ds0-group-no`
	Cisco 7200 Series Routers
	`Router(config)# voice-port slot/port-adapter:ds0-group-no`
	Cisco 7500 Series Routers
	`Router(config)# voice-port slot/port-adapter/slot:ds0-group-no`
		Enters voice-port configuration mode. The arguments are defined as the following
		• *slot*—Specifies the router location where the network module (Cisco 2600, 3600, and MC3810) or voice port adapter (Cisco AS5300, AS5800, 7200, and 7500) is installed. This is the same number as the controller for the T1/E1 voice port.
		• *port*—Indicates the voice interface card location.
		• *ds0-group-no*—Specifies the logical voice port that was created with the **ds0-group** controller command.
		• *controller*—Indicates the controller for the T1/E1 voice port.
		• *shelf*—Specifies the dial shelf, which is always 0.
		• *port-adapter*—Indicates the port adapter for the voice port.

Step 2	`Router(config-voiceport)# type {1 | 2 | 3 | 5}`	(E&M only) Specifies the type of E&M interface to which this voice port is connected. See Table 5 for an explanation of E&M types. The default is 1.

	Command	Purpose
Step 3	`Router(config-voiceport)# `**`cptone`** *`locale`*	Selects a two-letter **locale** keyword for the voice call progress tones and other locale-specific parameters to be used on this voice port. Voice call progress tones include dial tone, busy tone, and ringback tone, which vary with geographical region. Other parameters include ring cadence and compand type. Cisco routers comply with the ISO3166 locale name standards; to see valid choices, enter a question mark (?) following the **cptone** command. The default is **us**.
Step 4	`Router(config-voiceport)# `**`compand-type`**` {`**`u-law`**` | `**`a-law`**`}`	(Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators only) Specifies the companding standard used. This command is used in cases when the DSP is not used, such as local cross-connects, and overwrites the **compand-type** value set by the **cptone** command. The keywords are as follows: • **a-law**—Specifies the ITU-T PCM a-law companding standard used primarily in Europe. The default for E1 is **a-law**. • **u-law**—Specifies the ITU-T PCM mu-law companding standard used in North America and Japan. The default for T1 is **u-law**. **Note** If you have a Cisco MC3810 multiservice concentrator or Cisco 3660 router, the **compand-type a-law** command must be configured on the analog ports only. The Cisco 2660, 3620, and 3640 routers do not require the **compand-type a-law** command configured, however, if you request a list of commands, the **compand-type a-law** command will display.

Step 5	**Cisco 2600 series and 3600 series**
	`Router(config-voiceport)# `**`ring frequency`**` {25 | 50}`
	Cisco MC3810
	`Router(config-voiceport)# `**`ring frequency`**` {20 | 30}`
		(FXS only) Selects the ring frequency, in hertz, used on the FXS interface. This number must match the connected telephony equipment, and can be country-dependent. If not set properly, the attached telephony device may not ring or it may buzz.
		The default is 25 on the Cisco 2600 and 3600 series routers and 20 on the Cisco MC3810 multiservice concentrators.

7.334

	Command	Purpose
Step 6	Router(config-voiceport)# **ring number** *number*	(FXO only) Specifies the maximum number of rings to be detected before an incoming call is answered by the router. The default is 1.
Step 7	Router(config-voiceport)# **ring cadence** {[**pattern01** | **pattern02** | **pattern03** | **pattern04** | **pattern05** | **pattern06** | **pattern07** | **pattern08** | **pattern09** | **pattern10** | **pattern11** | **pattern12**] [**define** *pulse interval*]}	(FXS only) Specifies an existing pattern for ring, or defines a new one. Each pattern specifies a ring-pulse time and a ring-interval time. The keywords and arguments are as follows: • **pattern01** through **pattern12**—Specifies preset ring cadence patterns. Enter **ring cadence ?** to see ring pattern explanations. • **define** *pulse interval*—Specifies a user-defined pattern as follows: – *pulse* is a number (1 or 2 digits from 1 to 50) specifying ring pulse (on) time in hundreds of milliseconds. – *interval* is a number (1 or 2 digits from 1 to 50) specifying ring interval (off) time in hundreds of milliseconds. The default is the pattern specified by the configured **cptone locale** command.
Step 8	Router(config-voiceport)# **description** *string*	Attaches a text string to the configuration that describes the connection for this voice port. This description appears in various displays and is useful for tracking the purpose or use of the voice port. The *string* argument is a character string from 1 to 255 characters in length. The default is that no description is attached to the configuration.
Step 9	Router(config-voiceport)# **no shutdown**	Activates the voice port.

Fine-Tuning Analog and Digital Voice Ports

Normally, default parameter values for voice ports are sufficient for most networks. Depending on the specifics of your particular network, however, you may need to adjust certain parameters that are configured on voice ports. Collectively, these commands are referred to as voice port tuning commands.

Note The commands, keywords, and arguments that you are able to use may differ slightly from those presented here, based on your platform, Cisco IOS release, and configuration. When in doubt, use Cisco IOS command help (**command ?**) to determine the syntax choices that are available.

The voice port tuning commands are grouped into these categories and explained in the following sections:

- Auto Cut-Through Command, page 81
- Bit Modification Commands for Digital Voice Ports, page 81
- Calling Number Outbound Commands, page 83
- Disconnect Supervision Commands, page 84
- FXO Supervisory Disconnect Tone Commands, page 87
- Timeouts Commands, page 89
- Timing Commands, page 91
- DTMF Timer Inter-Digit Command for Cisco AS5300 Access Servers, page 92
- Voice Quality Tuning Commands, page 94

Full descriptions of the commands in this section can be found in the *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2.

Auto Cut-Through Command

The **auto-cut-through** command allows you to connect to PBXs that do not provide an M-lead response.

To configure auto-cut-through, use the following command in voice-port configuration mode:

Command	Purpose
`Router(config-voiceport)# **auto-cut-through**`	(E&M only) Enables call completion on a router when a PBX does not provide an M-lead response.

Bit Modification Commands for Digital Voice Ports

The bit modification commands for digital voice ports modify sent or received bit patterns. Different versions of E&M use different ABCD signaling bits to represent idle and seize. For example, North American CAS E&M represents idle as 0XXX and seize as 1XXX, where X indicates that the state of the BCD bits is ignored. In MELCAS E&M, idle is 1101 and seize is 0101. The commands in this section are provided to modify bit patterns to match particular E&M schemes.

To manipulate bit patterns for digital voice ports, use the following commands as necessary, in voice-port configuration mode:

7.332

<table>
<tr><th></th><th>Command</th><th>Purpose</th></tr>
<tr><td><b>Step 1</b></td><td><code>Router(config-voiceport)# <b>condition</b> {<b>tx-a-bit</b> | <b>tx-b-bit</b> | <b>tx-c-bit</b> | <b>tx-d-bit</b>} {<b>rx-a-bit</b> | <b>rx-b-bit</b> | <b>rx-c-bit</b> | <b>rx-d-bit</b>} {<b>on</b> | <b>off</b> | <b>invert</b>}</code></td><td>Manipulates sent or received bit patterns to match expected patterns on a connected device. Repeat the command for each transmit and/or receive bit to be modified, but be careful not to destroy the information content of the bit pattern.
The default is that the signaling format is not manipulated (for all transmit or receive A, B, C, and D bits).</td></tr>
<tr><td></td><td></td><td>The keywords are as follows:
• <b>on</b>—Sets the bit to 1 permanently.
• <b>off</b>—Sets the bit to 0 permanently.
• <b>invert</b>—Changes the state to the opposite of the original transmit or receive state.
<b>Note</b> The <b>show voice port</b> command reports at the protocol level, and the <b>show controller</b> command reports at the driver level. The driver is not notified of any bit manipulation using the <b>condition</b> command. As a result, the <b>show controller</b> command output does not account for the bit conditioning.</td></tr>
<tr><td><b>Step 2</b></td><td><code>Router(config-voiceport)# <b>define</b> {<b>tx-bits</b> | <b>rx-bits</b>} {<b>seize</b> | <b>idle</b>} {0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111}</code></td><td>(Digital E1 E&M voice ports on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators only) Defines specific transmit or receive signaling bits to match the bit patterns required by a connected device for North American E&M and E&M MELCAS voice signaling, if patterns different from the preset defaults are required.
Also specifies which bits a voice port monitors and which bits it ignores, if patterns that are different from the defaults are required.
See the <b>define</b> command for the default signaling patterns as defined in American National Standards Institute (ANSI) and code excited linear prediction compression (CEPT) standards. The keywords are as follows:
• <b>tx-bits</b>—Indicates the pattern applies to transmit signaling bits.</td></tr>
</table>

	Command	Purpose
		• **rx-bits**—Indicates the pattern applies to receive signaling bits • **seize**—Indicates that the pattern represents line seizure. • **idle**—Indicates that the pattern represents an idle condition. • **0000...1111**—Represents the bit pattern to use.
Step 3	`Router(config-voiceport)# ignore {rx-a-bit | rx-b-bit | rx-c-bit | rx-d-bit}`	(Digital E1 E&M voice ports on Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators only) Configures the voice port to ignore the specified receive bit for North American E&M or E&M MELCAS, if patterns different from the defaults are required. See the command reference for the default signaling patterns as defined in ANSI and CEPT standards.

Calling Number Outbound Commands

On the Cisco AS5300 universal access server platform, if T1 CAS is configured with the Feature Group-D (FGD)—Exchange Access North American (FGD-EANA) signaling, the automatic number identification (ANI) can be sent for outgoing calls by using the **calling-number outbound** command.

FGD-EANA is a FGD signaling protocol of type EANA, which provides certain call services, such as emergency (USA 911) calls. ANI is an SS7 (Signaling System 7) feature in which a series of digits, analog or digital, are included in the call to identify the telephone number of the calling device. In other words, ANI identifies the number of the calling party. ANI digits are used for billing purposes by Internet service providers (ISPs), among other things. The commands in this section can be issued in voice-port or dial-peer mode, because the syntax is the same.

To configure your digital T1/E1 packet voice trunk network module to generate outbound ANI digits on a Cisco AS5300 universal access server, use the following commands in voice-port configuration mode:

7.330

	Command	Purpose
Step 1	`Router(config-voiceport)# calling-number outbound range string1 string2`	(Cisco AS5300 universal access server only) Specifies ANI to be sent out when the T1-CAS **fgd-eana** command is configured as signaling type. The *string1* and *string2* arguments are valid E.164 telephone number strings. Both strings must be of the same length and cannot be more than 32 digits long. Only the last four digits are used for specifying the range (*string1* to *string2*) and for generating the sequence of ANI by rotating through the range until *string2* is reached and then starting from *string1* again. If strings are less than four digits in length, then entire strings are used.
Step 2	`Router(config-voiceport)# calling-number outbound sequence [string1] [string2] [string3] [string4] [string5]`	(Cisco AS5300 universal access server only) Specifies ANI to be sent out when the T1-CAS **fgd-eana** command is configured as signaling type. This option configures a sequence of discrete strings (*string1*...*string5*) to be passed out as ANI for successive calls using the dial peer or voice port. Limit is five (5) strings. All strings must be valid E.164 numbers, up to 32 digits in length.
Step 3	`Router(config-voiceport)# calling-number outbound null`	(Cisco AS5300 universal access server only) Suppresses ANI. No ANI is passed when this voice port is selected.

Disconnect Supervision Commands

PBX and PSTN switches use several different methods to indicate that a call should be disconnected because one or both parties have hung up. The commands in this section are used to configure the router to recognize the type of signaling in use by the PBX or PSTN switch connected to the voice port. These methods include the following:

- Battery reversal disconnect
- Battery denial disconnect
- Supervisory tone disconnect (STD)

Battery reversal occurs when the connected switch changes the polarity of the line in order to indicate changes in call state (such as off-hook or, in this case, call disconnect). This is the signaling looked for when the **battery reversal** command is enabled on the voice port, which is the default configuration.

Battery denial (sometimes called *power denial*) occurs when the connected switch provides a short (approximately 600 ms) interruption of line power to indicate a change in call state. This is the signaling looked for when the **supervisory disconnect** command is enabled on the voice port, which is the default configuration.

Supervisory tone disconnect occurs when the connected switch provides a special tone to indicate a change in call state. Some PBXs and PSTN CO switches provide a 600-millisecond interruption of line power as a supervisory disconnect, and others provide supervisory tone disconnect (STD). This is the signal that the router is looking for when the **no supervisory disconnect** command is configured on the voice port.

Note In some circumstances, you can use the FXO Disconnect Supervision feature to enable analog FXO ports to monitor call progress tones for disconnect supervision that are returned from a PBX or from the PSTN. For more information, see the "FXO Supervisory Disconnect Tone Commands" section on page 87.

7.328

To change parameters related to disconnect supervision, use the following commands as appropriate, in voice-port configuration mode:

	Command	Purpose
Step 1	`Router(config-voiceport)# no battery-reversal`	(Analog only) Enables battery reversal. The default is that battery reversal is enabled. • For FXO ports—Use the **no battery-reversal** command to configure a loop-start voice port not to disconnect when it detects a second battery reversal. The default is to disconnect when a second battery reversal is detected. This functionality is supported on Cisco MC3810 analog voice ports; on Cisco 1750, Cisco 2600 series, and Cisco 3600 series routers, only analog voice ports on VIC-2FXO cards are able to detect battery reversal. – Also use the **no battery-reversal** command when a connected FXO port does not support battery reversal detection. • For FXS ports—Use the **no battery-reversal** command to configure the voice port not to reverse battery when it connects calls. The default is to reverse battery when a call is connected, then return to normal when the call is over, providing positive disconnect. See also the **disconnect-ack** command (Step 7).
Step 2	`Router(config-voiceport)# no supervisory disconnect`	(FXO only) Enables the PBX or PSTN switch to provide STD. By default the **supervisory disconnect** command is enabled.
Step 3	`Router(config-voiceport)# disconnect-ack`	(FXS only) Configures the voice port to return an acknowledgment upon receipt of a disconnect signal. The FXS port removes line power if the equipment on the FXS loop-start trunk disconnects first. This is the default. The **no disconnect-ack** command prevents the FXS port from responding to the on-hook disconnect with a removal of line power.

7.327
J

FXO Supervisory Disconnect Tone Commands

If the FXO supervisory disconnect tone is configured and a detectable tone from the PSTN or PBX is detected by the digital signal processor (DSP), the analog FXO port goes on-hook. This feature prevents an analog FXO port from remaining in an off-hook state after an incoming call is ended. FXO supervisory disconnect tone enables interoperability with PSTN and PBX systems whether or not they transmit supervisory tones.

Note This feature applies only to analog FXO ports with loop-start signaling on the Cisco 2600 and 3600 series routers and on Cisco MC3810 multiservice concentrators with high-performance compression modules (HCMs).

To configure a voice port to detect incoming tones, you need to know the parameters of the tones expected from the PBX or PSTN. Then create a voice class that defines the tone detection parameters, and, finally, apply the voice class to the applicable analog FXO voice ports. This procedure configures the voice port to go on-hook when it detects the specified tones. The parameters of the tones need to be precisely specified to prevent unwanted disconnects due to detection of nonsupervisory tones or noise.

A supervisory disconnect tone is normally a dual tone consisting of two frequencies; however, tones of only one frequency can also be detected. Use caution if you configure voice ports to detect nondual tones, because unwanted disconnects can result from detection of random tone frequencies. You can configure a voice port to detect a tone with one on/off time cycle, or you can configure it to detect tones in a cadence pattern with up to four on/off time cycles.

Note In the following procedure, the following commands were not supported until Cisco IOS Release 12.2(2)T: **freq-max-deviation**, **freq-max-power**, **freq-min-power**, **freq-power-twist**, and **freq-max-delay**.

7.326

To create a voice class that defines the specific tone or tones to be detected and then apply the voice class to the voice port, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **`voice class dualtone`** *`tag`*	Creates a voice class for defining one tone detection pattern. The range for the tag number is from 1 to 10000. The tag number must be unique on the router. For more information about configuring voice classes, see the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter in this configuration guide.
Step 2	`Router(config-voice-class)#` **`freq-pair`** *`tone-id frequency-1 frequency-2`*	Specifies the two frequencies, in Hz, for a tone to be detected (or one frequency if a nondual tone is to be detected). If the tone to be detected contains only one frequency, enter 0 for *frequency-2*. The arguments are as follows: • *tone-id*—Ranges from 1 to 16. There is no default. • *frequency-1* and *frequency-2*—Ranges from 300 to 3600, or you can enter 0 for *frequency-2*. There is no default. **Note** Repeat this command for each additional tone to be specified.
Step 3	`Router(config-voice-class)#` **`freq-max-deviation`** *`frequency`*	Specifies the maximum frequency deviation that will be detected, in Hz. The *frequency* argument ranges from 10 to 125. The default is 10.
Step 4	`Router(config-voice-class)#` **`freq-max-power`** *`dBm0`*	Specifies the maximum tone power that will be detected, in dBmO. The *dBmO* argument ranges from 0 to 20. The default is 10.
Step 5	`Router(config-voice-class)#` **`freq-min-power`** *`dBm0`*	Specifies the minimum tone power that will be detected, in dBmO. The *dBmO* argument ranges from 10 to 35. The default is 30.
Step 6	`Router(config-voice-class)#` **`freq-power-twist`** *`dBm0`*	Specifies the power difference allowed between the two frequencies, in dBmO. The *dBmO* argument ranges from 0 to 15. The default is 6.
Step 7	`Router(config-voice-class)#` **`freq-max-delay`** *`time`*	Specifies the timing difference allowed between the two frequencies, in 10-millisecond increments. The *time* argument ranges from 10 to 100 (100 ms to 1 s). The default is 20 (200 ms).
Step 8	`Router(config-voice-class)#` **`cadence-min-on-time`** *`time`*	Specifies the minimum tone on time that will be detected, in 10-millisecond increments. The *time* argument ranges from 0 to 100 (0 ms to 1 s).
Step 9	`Router(config-voice-class)#` **`cadence-max-off-time`** *`time`*	Specifies the maximum tone off time that will be detected, in 10-millisecond increments. The *time* argument ranges from 0 to 5000 (0 ms to 50 s).

7.325

	Command	Purpose
Step 10	`Router(config-voice-class)# cadence-list cadence-id cycle-1-on-time cycle-1-off-time cycle-2-on-time cycle-2-off-time cycle-3-on-time cycle-3-off-time cycle-4-on-time cycle-4-off-time`	(Optional) Specifies a tone cadence pattern to be detected. Specify an on time and off time for each cycle of the cadence pattern. The arguments are as follows: • *cadence-id*—Ranges from 1 to 10. There is no default. • *cycle-N-on-time* and *cycle-N-off-time*—Range from 0 to 1000 (0 ms to 10 s). The default is 0.
Step 11	`Router(config-voice-class)# cadence-variation time`	(Optional) Specifies the maximum time that the tone onset can vary from the specified onset time and still be detected, in 10-millisecond increments. The *time* argument ranges from 0 to 200 (0 ms to 2 s). The default is 0.
Step 12	`Router(config-voice-class)# exit`	Exits voice class configuration mode.

Step 13	**Cisco 2600 and 3600 Series Routers**
	`Router(config)# voice-port slot/subunit/port`
	Cisco MC3810 Multiservice Concentrators
	`Router(config)# voice-port slot/port`
		Enters voice-port configuration mode.
		The arguments are as follows:
		• *slot*—Specifies the slot number where the voice network module is installed (Cisco 2600 and Cisco 3600 series routers) or the router slot number where the analog voice module is installed (Cisco MC3810 multiservice concentrators).
		• *subunit*—Specifies the voice interface card (VIC) where the voice port is located.
		• *port*—Identifies the analog voice-port number.

Step 14	`Router(config-voiceport)# supervisory disconnect dualtone {mid-call | pre-connect} voice-class tag`	Assigns an FXO supervisory disconnect tone voice class to the voice port. The keywords are as follows: • **mid-call**—Specifies tone detection during the entire call. • **pre-connect**—Specifies tone detection only during call set-up.
Step 15	`Router(config-voiceport)# supervisory disconnect anytone`	Configures the voice port to disconnect on receipt of any tone.

Timeouts Commands

To change timeouts parameters, use the following commands as appropriate, in voice-port configuration mode:

7.324

	Command	Purpose
Step 1	`Router(config-voiceport)#` **`timeouts call-disconnect`** *`seconds`*	Configures the call disconnect timeout value in seconds. Valid entries range from 0 to 120. The default is 60.
Step 2	`Router(config-voiceport)#` **`timeouts initial`** *`seconds`*	Sets the number of seconds that the system waits between the caller input of the initial digit and the subsequent digit of the dialed string. If the wait time expires before the destination is identified, a tone sounds and the call ends. The *seconds* argument is the initial timeout duration. A valid entry is an integer from 0 to 120. The default is 10.
Step 3	`Router(config-voiceport)#` **`timeouts interdigit`** *`seconds`*	Configures the number of seconds that the system waits after the caller has input the initial digit or a subsequent digit of the dialed string. If the timeout ends before the destination is identified, a tone sounds and the call ends. This value is important when using variable-length dial peer destination patterns (dial plans). The *seconds* argument is the interdigit timeout wait time in seconds. A valid entry is an integer from 0 to 120. The default is 10.
Step 4	`Router(config-voiceport)#` **`timeouts ringing`** `{`*`seconds`* `|` **`infinity`**`}`	Specifies the duration that the voice port allows ringing to continue if a call is not answered. The keyword and argument are as follows: • **infinity**—Indicates ringing should continue until the caller goes on hook. • *seconds*—Specifies the number of seconds to allow ringing without answer. The range is from 5 to 60000. The default is 180.
Step 5	`Router(config-voiceport)#` **`timeouts wait-release`** `{`*`seconds`* `|` **`infinity`**`}`	Specifies the duration that a voice port stays in the call-failure state while the Cisco device sends busy tone, reorder tone, or an out-of-service to the port. The keyword and argument are as follows: • **infinity**—Indicates the voice port should not be released as long as the call-failure state remains. • *seconds*—Specifies the number of seconds to allow before the call is released. The range is from 3 to 3600. The default is 30.

7.323
J

Timing Commands

To change timing parameters, use the following commands as appropriate, in voice-port configuration mode:

	Command	Purpose
Step 1	Router(config-voiceport)# **timing clear-wait** *milliseconds*	(E&M only) Specifies the minimum amount of time between the inactive seizure signal and clearing of the call. Valid entries for the *milliseconds* argument are from 200 to 2000 milliseconds. The default is 400.
Step 2	Router(config-voiceport)# **timing delay-duration** *milliseconds*	(E&M only) Specifies the delay signal duration for delay-dial signaling in milliseconds. Valid entries are from 100 to 5000. The default is 2000.
Step 3	Router(config-voiceport)# **timing delay-start** *milliseconds*	(E&M only) Specifies minimum delay time, in milliseconds, from outgoing seizure to outdial address. Valid entries are from 20 to 2000. The default is 300 for the Cisco 3600 series routers, and 150 for the Cisco MC3810 multiservice concentrators.
Step 4	Router(config-voiceport)# **timing delay-with-integrity** *milliseconds*	(Cisco MC3810 multiservice concentrators E&M ports only) Specifies duration of the wink pulse for the delay dial in milliseconds. Valid entries are from 0 to 5000. The default is 0.
Step 5	Router(config-voiceport)# **timing dial-pulse min-delay** *milliseconds*	Specifies time, in milliseconds, between the generation of wink-like pulses when the type is pulse. Valid entries are from 0 to 5000. The default is 300 for the Cisco 3600 series routers, and 140 for the Cisco MC3810 multiservice concentrators.
Step 6	Router(config-voiceport)# **timing dialout-delay** *milliseconds*	(Cisco MC3810 multiservice concentrators only) Specifies dialout delay, in milliseconds, for the sending digit or cut-through on an FXO trunk or an E&M immediate trunk. Valid entries are from 100 to 5000. The default is 300.
Step 7	Router(config-voiceport)# **timing digit** *milliseconds*	Specifies the DTMF digit signal duration in milliseconds. Valid entries are from 50 to 100. The default is 100.
Step 8	Router(config-voiceport)# **timing guard-out** *milliseconds*	(FXO ports only) Specifies the duration in milliseconds of the guard-out period that prevents this port from seizing a remote FXS port before the remote port detects a disconnect signal. The range is from 300 to 3000. The default is 2000.
Step 9	Router(config-voiceport)# **timing hookflash-out** *milliseconds*	Specifies the duration, in milliseconds, of the hookflash. Valid entries are from 50 to 500. The default is 300.

7.322

	Command	Purpose
Step 10	Router(config-voiceport)# **timing interdigit** *milliseconds*	Specifies the DTMF interdigit duration, in milliseconds. Valid entries are from 50 to 500. The default is 100.
Step 11	Router(config-voiceport)# **timing percentbreak** *percent*	(Cisco MC3810 multiservice concentrators FXO and E&M ports only) Specifies the percentage of the break period for the dialing pulses, if different from the default. The range is from 20 to 80. The default is 50.
Step 12	Router(config-voiceport)# **timing pulse** *pulses-per-second*	(FXO and E&M only) Specifies the pulse dialing rate in pulses per second. Valid entries are from 10 to 20. The default is 20.
Step 13	Router(config-voiceport)# **timing pulse-digit** *milliseconds*	(FXO only) Configures the pulse digit signal duration. The range of the pulse digit signal duration is from 10 to 20. The default is 20.
Step 14	Router(config-voiceport)# **timing pulse-interdigit**	(FXO and E&M only) Specifies pulse dialing interdigit timing in milliseconds. Valid entries are from 100 to 1000. The default is 500.
Step 15	Router(config-voiceport)# **timing wink-duration** *milliseconds*	(E&M only) Specifies maximum wink-signal duration, in milliseconds, for a wink-start signal. Valid entries are from 100 to 400. The default is 200.
Step 16	Router(config-voiceport)# **timing wink-wait** *milliseconds*	(E&M only) Specifies maximum wink-wait duration, in milliseconds, for a wink-start signal. Valid entries are from 100 to 5000. The default is 200.

DTMF Timer Inter-Digit Command for Cisco AS5300 Access Servers

To configure the DTMF timer for Cisco AS5300 access servers, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **controller T1** *number*	Configures a T1 controller and enters controller configuration mode.
Step 2	Router(config)# **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type* **dtmf dnis**	Configures channelized T1 timeslots, which enables a Cisco AS5300 modem to answer and send an analog call.
Step 3	Router(config)# **cas-custom** *channel*	Customizes E1 R2 signaling parameters for a particular E1 channel group on a channelized E1 line.
Step 4	Router(conf-ctrl-cas)# **dtmf-timer-inter-digit** *milliseconds*	Configures the DTMF inter-digit timer for a DS0 group.

7.321

Verifying DTMF Timer Inter-Digit Command

To verify the DTMF timer, use the following command in EXEC mode:

Command	Purpose
`Router# show running-config`	Displays the configuration information currently running on the terminal.

Voice Activity Detection Commands Related to Voice-Port Configuration Mode

In normal voice conversations, only one person speaks at a time. Today's circuit-switched telephone networks dedicate a bidirectional, 64 kbps channel for the duration of each conversation, regardless of whether anyone is speaking at the moment. This means that, in a normal voice conversation, at least 50 percent of the bandwidth is wasted when one or both parties are silent. This figure can actually be much higher when normal pauses and breaks in conversation are taken into account.

Packet-switched voice networks, on the other hand, can use this "wasted" bandwidth for other purposes when voice activity detection (VAD) is configured. VAD works by detecting the magnitude of speech in decibels and deciding when to cut off the voice from being framed. VAD has some technological problems, however, which include the following:

- General difficulties determining when speech ends
- Clipped speech when VAD is slow to detect that speech is beginning again
- Automatic disabling of VAD when conversations take place in noisy surroundings

VAD is configured on dial peers; by default it is enabled. For more information, see the "Configuring Dial Plans, Dial Peers, and Digit Manipulation" chapter in this configuration guide. Two parameters associated with VAD, music threshold and comfort noise, are configured on voice ports.

If VAD is enabled, use the following commands to adjust parameter values associated with VAD, beginning in voice-port configuration mode:

	Command	Purpose
Step 1	`Router(config-voiceport)# music-threshold number`	Specifies the minimal decibel level of music played when calls are put on hold. The decibel level affects how voice activity detection (VAD) treats the music data. Valid entries range from –70 to –30. When used with VAD, if the level is set too high, the remote end hears no music; if it is set too low, there is unnecessary voice traffic. The default is –38.
Step 2	`Router(config-voiceport)# comfort-noise`	This parameter creates subtle background noise to fill silent gaps during calls when VAD is enabled on voice dial peers. If comfort noise is not generated, the resulting silence can fool the caller into thinking the call is disconnected instead of being merely idle. The default is that comfort noise is enabled.

7.320

Voice Quality Tuning Commands

The commands in this section configure parameters to improve voice quality. Common voice quality issues include the following:

- Delay in Voice Networks
- Jitter Adjustment
- Echo Adjustment
- Voice Level Adjustment

Delay in Voice Networks

Delay is the time it takes for voice packets to travel between two endpoints. Excessive delay can cause quality problems with real-time traffic such as voice. However, because of the speed of network links and the processing power of intermediate devices, some delay is expected.

When listening to speech, the human ear normally accepts up to about 150 ms of delay without noticing delays. The ITU G.114 standard recommends no more than 150 ms of one-way delay for a normal voice conversation. Once the delay exceeds 150 ms, a conversation is more like a "walkie-talkie" conversation in which one person must wait for the other to stop speaking before beginning to talk.

You can measure delay fairly easily by using ping tests at various times of the day with different network traffic loads. If network delay is excessive, it must be reduced for adequate voice quality.

Several different types of delay combine to make up the total end-to-end delay associated with voice calls:

- Propagation delay—Amount of time it takes the data to physically travel over the media.
- Handling delay—Amount of time it takes to process data by adding headers, taking samples, forming packets, etc.
- Queuing delay—Amount of time lost due to congestion.
- Variable delay or jitter—Amount of time that causes the conversation to break and become unintelligible. Jitter is described in detail below.

Propagation, handling, and queuing delay are not addressed by voice-port commands and fall outside the scope of this chapter.

Jitter Adjustment

Delay can cause unnatural starting and stopping of conversations, but variable-length delays (also known as jitter) can cause a conversation to break and become unintelligible. Jitter is not usually a problem with PSTN calls because the bandwidth of calls is fixed and each call has a dedicated circuit for the duration of the call. However, in VoIP networks, data traffic might be bursty, and jitter from the packet network can become an issue. Especially during times of network congestion, packets from the same conversation can arrive at different interpacket intervals, disrupting the steady, even delivery needed for voice calls. Cisco voice gateways have built-in jitter buffering to compensate for a certain amount of jitter; the **playout-delay** command can be used to adjust the jitter buffer.

Normally, the defaults in effect are sufficient for most networks. However, a small playout delay from the jitter buffer can cause lost packets and choppy audio, and a large playout delay can cause unacceptably high overall end-to-end delay.

7.319

Note Prior to Cisco IOS Release 12.1(5)T, playout delay was configured in voice-port configuration mode. For Cisco IOS Release 12.1(5)T and later releases, in most cases playout delay should be configured in dial-peer configuration mode on the VoIP dial peer that is on the receiving end of the voice traffic that is to be buffered. This dial peer senses network conditions and relays them to the DSPs, which adjust the jitter buffer as necessary. When multiple applications are configured on the gateway, playout delay should be configured in dial-peer configuration mode. When there are numerous dial peers to configure, it might be simpler to configure playout delay on a voice port. If there are conflicting playout delay configurations on a voice port and also on a dial peer, the dial peer configuration takes precedence.

To configure the playout delay jitter buffer, use the following commands beginning in dial-peer or voice-port configuration mode:

	Command	Purpose
Step 1	`Router(config-voiceport)# playout-delay mode {adaptive | fixed}`	Determines the mode in which the jitter buffer will operate for calls on this voice port. The keywords are as follows: • **adaptive**—Adjusts the jitter buffer size and amount of playout delay during a call based on current network conditions. • **fixed**—Defines the jitter buffer size as fixed so that the playout delay does not adjust during a call. A constant playout delay is added. The default is **adaptive**.

7.3.8

	Command	Purpose
Step 2	`Router(config-voiceport)# playout-delay {nominal value | maximum value | minimum {default | low | high}}`	Tunes the playout buffer to accommodate packet jitter caused by switches in the WAN. The keywords and arguments are as follows: • **nominal**—Defines the amount of playout delay applied at the beginning of a call by the jitter buffer in the gateway. In fixed mode, this is also the maximum size of the jitter buffer throughout the call. • *value*—Specifies the range that depends on type of DSP and configured codec complexity. For medium codec complexity, the range is from 0 to 150 ms. For high codec complexity and DSPs that do not support codec complexity, the range is from 0 to 250 ms. • **maximum** (adaptive mode only)—Specifies the jitter buffer's upper limit (80ms), or the highest value to which the adaptive delay is set. • **minimum** (adaptive mode only)—Specifies the jitter buffer's lower limit (10 ms), or the lowest value to which the adaptive delay is set. • **default**—Specifies 40 ms.

Echo Adjustment

Echo is the sound of your own voice reverberating in the telephone receiver while you are talking. When timed properly, echo is not a problem in the conversation; however, if the echo interval exceeds approximately 25 milliseconds, it is distracting. Echo is controlled by echo cancellers.

In the traditional telephony network, echo is generally caused by an impedance mismatch when the four-wire network is converted to the two-wire local loop. In voice packet-based networks, echo cancellers are built into the low-bit rate codecs and are operated on each DSP.

By design, echo cancellers are limited by the total amount of time they wait for the reflected speech to be received, which is known as an echo trail. The echo trail is normally 32 milliseconds. In Cisco System's voice implementations, echo cancellers are enabled using the **echo-cancel enable** command, and echo trails are configured using the **echo-cancel coverage** command.

To configure parameters related to the echo canceller, use the following commands beginning in voice-port configuration mode:

	Command	Purpose
Step 1	`Router(config-voiceport)# echo-cancel enable`	Enables the cancellation of voice that is sent and received on the same interface. Echo cancellation coverage must also be configured. The default is that echo cancellation is enabled. **Note** Not valid for four-wire E&M interfaces. Use **no echo-cancel enable** to disable the feature.
Step 2	`Router(config-voiceport)# echo-cancel coverage {8 | 16 | 24 | 32}`	Adjusts the echo canceller by the specified number of milliseconds. The default is 16.
Step 3	`Router(config-voiceport)# non-linear`	Enables nonlinear processing (residual echo suppression) in the echo canceler, which shuts off any signal if no near-end speech is detected. Echo cancelling must be enabled for this feature. The default is that nonlinear processing is enabled.

7.316

Voice Level Adjustment

As much as possible, it is desirable to achieve a uniform input decibel level to the packet voice network in order to limit or eliminate any voice distortion due to incorrect input and output decibel levels. Adjustments to levels may be required by the type of equipment connected to the network or by local country-specific conditions.

Incorrect input or output levels can cause echo, as can an impedance mismatch. Too much input gain can cause clipped or fuzzy voice quality. If the output level is too high at the remote router's voice port, the local caller will hear echo. If the local router's voice port input decibel level is too high, the remote side will hear clipping. If the local router's voice port input decibel level is too low, or the remote router's output level is too low, the remote side voice can be distorted at a very low volume and DTMF may be missed.

Use the **input gain** and **output attenuation** commands to adjust voice levels, and the **impedance** command to set the impedance value to match that of the voice circuit to which the voice port connects.

To change parameters related to voice levels, use the following commands as appropriate, in voice-port configuration mode:

	Command	Purpose
Step 1	Router(config-voiceport)# **input gain** *value*	Specifies, in decibels, the amount of gain to be inserted at the receiver side of the interface, increasing or decreasing the signal. After an input gain setting is changed, the voice call must be disconnected and reestablished before the changes take effect. The *value* argument is any integer from –6 to 14. The default is 0.
Step 2	Router(config-voiceport)# **output attenuation** *value*	Specifies the amount of attenuation in decibels at the transmit side of the interface, decreasing the signal. A system-wide loss plan can be implemented using the **input gain** and **output attenuation** commands. The default value for this command assumes that a standard transmission loss plan is in effect, meaning that normally there must be –6 dB attenuation between phones. The *value* argument is any integer from –6 to 14. The default is 0.
Step 3	Router(config-voiceport)# **impedance** {**600c** | **600r** | **900c** | **complex1** | **complex2**}	Specifies the terminating impedance of a voice port interface, which needs to match the specifications from the specific telephony system to which it is connected. • **600c**—Specifies 600 ohms complex. • **600r**—Specifies 600 ohms real. • **900c**—Specifies 900 ohms complex. • **complex1**—Specifies Complex 1. • **complex2**—Specifies Complex 2. The default is 600r.

	Command	Purpose
Step 4	`Router(config-voiceport)# loss-plan {plan1 | plan2 | plan5 | plan6 | plan7 | plan8 | plan9}`	(Cisco MC3810 multiservice concentrators FXO or FXS analog voice ports only) Specifies the analog-to-digital gain offset loss plan. For definitions of each plan, see the *Cisco IOS Voice, Video, and Fax Command Reference*. The default is the **plan1** keyword.
Step 5	`Router(config-voiceport)# idle-voltage {high | low}`	(Cisco MC3810 multiservice concentrators analog FXS ports only) Specifies the talk-battery (tip-to-ring) voltage condition when the port is idle. The keywords are as follows: • **high**—Specifies that the voltage is high (–48V). • **low**—Specifies that the voltage is low (–24V) and is the default.

Verifying Analog and Digital Voice-Port Configurations

After configuring the voice ports on your router, perform the following steps to verify proper operation:

Step 1 Pick up the handset of an attached telephony device and check for a dial tone.

Step 2 If you have dial tone, check for DTMF detection. If the dial tone stops when you dial a digit, then the voice port is most likely configured properly.

Step 3 To identify port numbers of voice interfaces installed in your router, use the **show voice port summary** command. For examples of the output, see the "show voice port summary Command Examples" section on page 100.

Step 4 To verify voice-port parameter settings, use the **show voice port** command with the appropriate syntax from Table 9. For sample output, see the "show voice port Command Examples" section on page 101.

Table 9 Show Voice Port Command Syntax

Platform	Voice Port Type	Command Syntax
Cisco 1750	Analog	**show voice port** [*slot/port* | **summary**]
Cisco 2600 series Cisco 3600 series	Analog	**show voice port** [*slot/port* | **summary**]
	Digital	**show voice port** [*slot/port:ds0-group-no* | **summary**]
Cisco MC3810	Analog	**show voice port** [*slot/port* | **summary**]
	Digital	**show voice port** [*slot:ds0-group-no* | **summary**]
Cisco AS5300	Digital	**show voice-port** *controller:ds0-group-no*
Cisco AS5800	Digital	**show voice-port** {*shelf/slot/port:ds0-group-no*}
Cisco 7200 series	Digital	**show voice port** {*slot/port-adapter:ds0-group-no*}
Cisco 7500 series	Digital	**show voice port** {*slot/port-adapter/slot:ds0-group-no*}

7.34 >

Step 5 For digital T1/E1 connections, to verify the codec complexity configuration, use the **show running-config** command to display the current voice-card setting. If medium complexity is specified, the codec complexity setting is not displayed. If high complexity is specified, the setting codec complexity high is displayed. The following example shows an excerpt from the command output when high complexity has been specified:

```
Router# show running-config
.
.
.
hostname router-alpha

voice-card 0
 codec complexity high
.
.
.
```

Step 6 For digital T1/E1 connections, to verify that the controller is up and that no alarms have been reported, and to display information about clock sources and other controller settings, use the **show controller** command. For output examples, see the "show controller Command Examples" section on page 105.

```
Router# show controller {t1 | e1} controller-number
```

Step 7 To display voice-channel configuration information for all DSP channels, use the **show voice dsp** command. For output examples, see the "show voice dsp Command Examples" section on page 106.

```
Router# show voice dsp
```

Step 8 To verify the call status for all voice ports, use the **show voice call summary** command. For output examples, see the "show voice call summary Command Examples" section on page 107.

```
Router# show voice call summary
```

Step 9 To display the contents of the active call table, which shows all of the calls currently connected through the router or concentrator, use the **show call active voice** command. For output examples, see the "show call active voice Command Example" section on page 107.

```
Router# show call active voice
```

Step 10 To display the contents of the call history table, use the **show call history voice** command. To limit the display to the last calls connected through this router, use the keyword **last** and define the number of calls to be displayed with the argument *number*. To limit the display to a shortened version of the call history table, use the **brief** keyword. For output examples, see the "show call history voice Command Example" section on page 108.

```
Router# show call history voice [last | number | brief]
```

show voice port summary Command Examples

In the following sections, output examples of the following types are shown:

- Cisco 3640 Router Analog Voice Port
- Cisco MC3810 Multiservice Concentrator Digital Voice Port

Cisco 3640 Router Analog Voice Port

The following output is from a Cisco 3640 router:

```
Router# show voice port summary
                                      IN        OUT
PORT    CH SIG-TYPE   ADMIN OPER STATUS    STATUS   EC
====== == ========== ===== ==== ======== ======== ==
2/0/0   -- e&m-wnk    up    dorm idle      idle     y
2/0/1   -- e&m-wnk    up    dorm idle      idle     y
2/1/0   -- fxs-ls     up    dorm on-hook   idle     y
2/1/1   -- fxs-ls     up    dorm on-hook   idle     y
```

Cisco MC3810 Multiservice Concentrator Digital Voice Port

The following output is from a Cisco MC3810 multiservice concentrator:

```
Router# show voice port summary
                                      IN        OUT
PORT    CH SIG-TYPE   ADMIN OPER STATUS    STATUS   EC
====== == ========== ===== ==== ======== ======== ==
0:17    18 fxo-ls     down  down idle      on-hook  y
0:18    19 fxo-ls     up    dorm idle      on-hook  y
0:19    20 fxo-ls     up    dorm idle      on-hook  y
0:20    21 fxo-ls     up    dorm idle      on-hook  y
0:21    22 fxo-ls     up    dorm idle      on-hook  y
0:22    23 fxo-ls     up    dorm idle      on-hook  y
0:23    24 e&m-imd    up    dorm idle      idle     y
1/1     -- fxs-ls     up    dorm on-hook   idle     y
1/2     -- fxs-ls     up    dorm on-hook   idle     y
1/3     -- e&m-imd    up    dorm idle      idle     y
1/4     -- e&m-imd    up    dorm idle      idle     y
1/5     -- fxo-ls     up    dorm idle      on-hook  y
1/6     -- fxo-ls     up    dorm idle      on-hook  y
```

show voice port Command Examples

In the following sections, output examples of the following types are shown:

- Cisco 3600 Series Router Analog E&M Voice Port, page 101
- Cisco 3600 Series Router Analog FXS Voice Port, page 102
- Cisco 3600 Series Router Digital E&M Voice Port, page 103
- Cisco AS5300 Universal Access Server T1 CAS Voice Port, page 103
- Cisco 7200 Series Router Digital E&M Voice Port, page 104

Cisco 3600 Series Router Analog E&M Voice Port

The following output is from a Cisco 3600 series router analog E&M voice port:

```
Router# show voice port 1/0/0

E&M Slot is 1, Sub-unit is 0, Port is 0
 Type of VoicePort is E&M
 Operation State is unknown
 Administrative State is unknown
 The Interface Down Failure Cause is 0
 Alias is NULL
```

7.3.2

```
Noise Regeneration is disabled
Non Linear Processing is disabled
Music On Hold Threshold is Set to 0 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is disabled
Echo Cancel Coverage is set to 16ms
Connection Mode is Normal
Connection Number is
Initial Time Out is set to 0 s
Interdigit Time Out is set to 0 s
Analog Info Follows:
Region Tone is set for northamerica
Currently processing none
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0

Voice card specific Info Follows:
Signal Type is wink-start
Operation Type is 2-wire
Impedance is set to 600r Ohm
E&M Type is unknown
Dial Type is dtmf
In Seizure is inactive
Out Seizure is inactive
Digit Duration Timing is set to 0 ms
InterDigit Duration Timing is set to 0 ms
Pulse Rate Timing is set to 0 pulses/second
InterDigit Pulse Duration Timing is set to 0 ms
Clear Wait Duration Timing is set to 0 ms
Wink Wait Duration Timing is set to 0 ms
Wink Duration Timing is set to 0 ms
Delay Start Timing is set to 0 ms
Delay Duration Timing is set to 0 ms
```

Cisco 3600 Series Router Analog FXS Voice Port

The following output is from a Cisco 3600 series router analog FXS voice port:

```
Router# show voice port 1/2

Voice port 1/2 Slot is 1, Port is 2
 Type of VoicePort is FXS
 Operation State is UP
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 8 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Coder Type is g729ar8
 Companding Type is u-law
 Voice Activity Detection is disabled
 Ringing Time Out is 180 s
 Wait Release Time Out is 30 s
 Nominal Playout Delay is 80 milliseconds
```

```
Maximum Playout Delay is 160 milliseconds

Analog Info Follows:
Region Tone is set for northamerica
Currently processing Voice
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Impedance is set to 600r Ohm
Analog interface A-D gain offset = -3 dB
Analog interface D-A gain offset = -3 dB
Voice card specific Info Follows:
Signal Type is loopStart
Ring Frequency is 20 Hz
Hook Status is On Hook
Ring Active Status is inactive
Ring Ground Status is inactive
Tip Ground Status is active
Digit Duration Timing is set to 100 ms
InterDigit Duration Timing is set to 100 ms
Ring Cadence are [20 40] * 100 msec
InterDigit Pulse Duration Timing is set to 500 ms
```

Cisco 3600 Series Router Digital E&M Voice Port

The following output is from a Cisco 3600 series router digital E&M voice port:

```
Router# show voice port 1/0:1

receEive and transMit Slot is 1, Sub-unit is 0, Port is 1
 Type of VoicePort is E&M
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 8 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Region Tone is set for US
```

Cisco AS5300 Universal Access Server T1 CAS Voice Port

The following output is from a Cisco AS5300 universal access server T1 CAS voice port:

```
Router# show voice port

DS0 Group 1:0 - 1:0
 Type of VoicePort is CAS
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 dBm
```

```
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 8 ms
Playout-delay Mode is set to default
Playout-delay Nominal is set to 60 ms
Playout-delay Maximum is set to 200 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Call-Disconnect Time Out is set to 60 s
Ringing Time Out is set to 180 s
Companding Type is u-law
Region Tone is set for US
Wait Release Time Out is 30 s
Station name None, Station number None

Voice card specific Info Follows:

DS0 channel specific status info:
                              IN      OUT
   PORT    CH SIG-TYPE    OPER STATUS  STATUS     TIP      RING
```

7.310

Cisco 7200 Series Router Digital E&M Voice Port

The following output is from a Cisco 7200 series router digital E&M voice port:

```
Router# show voice port 1/0:1

receEive and transMit Slot is 1, Sub-unit is 0, Port is 1  << voice-port 1/0:1

 Type of VoicePort is E&M

 Operation State is DORMANT

 Administrative State is UP

 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB

 Out Attenuation is Set to 0 dB

 Echo Cancellation is enabled

 Echo Cancel Coverage is set to 8 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s

 Interdigit Time Out is set to 10 s

 Region Tone is set for US
```

show controller Command Examples

In the following sections, output examples of the following types are shown:

- Cisco 3600 Series Router T1 Controller, page 105
- Cisco MC3810 Multiservice Concentrator E1 Controller, page 105
- Cisco AS5800 Universal Access Server T1 Controller, page 105

Cisco 3600 Series Router T1 Controller

The following output is from a Cisco 3600 series router with a T1 controller:

```
Router# show controller T1 1/1/0

T1 1/0/0 is up.
  Applique type is Channelized T1
  Cablelength is long gain36 0db
  No alarms detected.
  alarm-trigger is not set
  Framing is ESF, Line Code is B8ZS, Clock Source is Line.
  Data in current interval (180 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Cisco MC3810 Multiservice Concentrator E1 Controller

The following output is from a Cisco MC3810 multiservice concentrator with an E1 controller:

```
Router# show controller E1 1/0

E1 1/0 is up.
  Applique type is Channelized E1
  Cablelength is short 133
  Description: E1 WIC card Alpha
  No alarms detected.
  Framing is CRC4, Line Code is HDB3, Clock Source is Line Primary.
  Data in current interval (1 seconds elapsed):
     0 Line Code Violations, 0 Path Code Violations
     0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
     0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Cisco AS5800 Universal Access Server T1 Controller

The following output is from a Cisco AS5800 universal access server with a T1 controller:

```
Router# show controller t1 2

 T1 2 is up.
   No alarms detected.
   Version info of slot 0:  HW: 2, Firmware: 16, PLD Rev: 0

 Manufacture Cookie Info:
  EEPROM Type 0x0001, EEPROM Version 0x01, Board ID 0x42,
  Board Hardware Version 1.0, Item Number 73-2217-4,
  Board Revision A0, Serial Number 06467665,
  PLD/ISP Version 0.0, Manufacture Date 14-Nov-1997.

   Framing is ESF, Line Code is B8ZS, Clock Source is Internal.
```

```
Data in current interval (269 seconds elapsed):
 0 Line Code Violations, 0 Path Code Violations
   0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
   0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

7.308

show voice dsp Command Examples

The following output is from a Cisco 3640 router when a digital voice port is configured:

```
Router# show voice dsp

TYPE DSP CH CODEC    VERS STATE STATE   RST AI PORT    TS ABORT   TX/RX-PAK-CNT
==== === == ======== ==== ===== ======= === == ======= == ===== ===============
C549 010 00 g729r8    3.3 busy  idle      0  0 1/015    1     0     67400/85384
         01 g729r8     .8 busy  idle      0  0 1/015    7     0     67566/83623
         02 g729r8        busy  idle      0  0 1/015   13     0     65675/81851
         03 g729r8        busy  idle      0  0 1/015   20     0     65530/83610
C549 011 00 g729r8    3.3 busy  idle      0  0 1/015    2     0     66820/84799
         01 g729r8     .8 busy  idle      0  0 1/015    8     0     59028/66946
         02 g729r8        busy  idle      0  0 1/015   14     0     65591/81084
         03 g729r8        busy  idle      0  0 1/015   21     0     66336/82739
C549 012 00 g729r8    3.3 busy  idle      0  0 1/015    3     0     59036/65245
         01 g729r8     .8 busy  idle      0  0 1/015    9     0     65826/81950
         02 g729r8      . busy  idle      0  0 1/015   15     0     65606/80733
         03 g729r8        busy  idle      0  0 1/015   22     0     65577/83532
C549 013 00 g729r8    3.3 busy  idle      0  0 1/015    4     0     67655/82974
         01 g729r8     .8 busy  idle      0  0 1/015   10     0     65647/82088
         02 g729r8        busy  idle      0  0 1/015   17     0     66366/80894
         03 g729r8        busy  idle      0  0 1/015   23     0     66339/82628
C549 014 00 g729r8    3.3 busy  idle      0  0 1/015    5     0     68439/84677
         01 g729r8     .8 busy  idle      0  0 1/015   11     0     65664/81737
         02 g729r8        busy  idle      0  0 1/015   18     0     65607/81820
         03 g729r8        busy  idle      0  0 1/015   24     0     65589/83889
C549 015 00 g729r8    3.3 busy  idle      0  0 1/015    6     0     66889/83331
         01 g729r8     .8 busy  idle      0  0 1/015   12     0     65690/81700
         02 g729r8        busy  idle      0  0 1/015   19     0     66422/82099
         03 g729r8        busy  idle      0  0 1/015   25     0     65566/83852

Router# show voice dsp

TYPE DSP CH CODEC    VERS STATE STATE   RST AI PORT    TS ABORT   TX/RX-PAK-CNT
==== === == ======== ==== ===== ======= === == ======= == ===== ===============
C549 007 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    4     0             0/0
                      .13
C549 008 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    5     0             0/0
                      .13
C549 009 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    6     0             0/0
                      .13
C549 010 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    7     0             0/0
                      .13
C549 011 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    8     0             0/0
                      .13
C549 012 00 {medium}  3.3 IDLE  idle      0  0 1/0:1    9     0             0/0
                      .13
C542 001 01 g711ulaw  3.3 IDLE  idle      0  0 2/0/0           0         512/519
                      .13
C542 002 01 g711ulaw  3.3 IDLE  idle      0  0 2/0/1           0         505/502
                      .13
C542 003 01 g711alaw  3.3 IDLE  idle      0  0 2/1/0           0     28756/28966
                      .13
C542 004 01 g711ulaw  3.3 IDLE  idle      0  0 2/1/1           0         834/838
                      .13
```

7.307
J

show voice call summary Command Examples

In the following sections, output examples of the following types are shown:

- Cisco MC3810 Multiservice Concentrator Analog Voice Port
- Cisco 3600 Series Router Digital Voice Port

Cisco MC3810 Multiservice Concentrator Analog Voice Port

The following output is from a Cisco MC3810 multiservice concentrator:

```
Router# show voice call summary

PORT      CODEC    VAD VTSP STATE            VPM STATE
========= ======== === ==================== =======================
1/1       g729r8    y  S_CONNECT            FXSLS_CONNECT
1/2       -         -  -                    FXSLS_ONHOOK
1/3       -         -  -                    EM_ONHOOK
1/4       -         -  -                    EM_ONHOOK
1/5       -         -  -                    FXOLS_ONHOOK
1/6       -         -  -                    FXOLS_ONHOOK
```

Cisco 3600 Series Router Digital Voice Port

The following output is from a Cisco 3600 series router:

```
Router# show voice call summary

PORT      CODEC    VAD VTSP STATE            VPM STATE
========= ======== === ==================== =======================
1/015.1  g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.2  g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.3  g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.4  g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.5  g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.6  g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.7  g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.8  g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.9  g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.10 g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.11 g729r8    y  S_CONNECT            S_TSP_CONNECT
1/015.12 g729r8    y  S_CONNECT            S_TSP_CONNECT
```

show call active voice Command Example

The following output is from a Cisco 7200 series router:

```
Router# show call active voice

GENERIC:
SetupTime=94523746 ms
Index=448
PeerAddress=##73072

PeerSubAddress=
PeerId=70000

PeerIfIndex=37
```

7.306

```
LogicalIfIndex=0
ConnectTime=94524043
DisconectTime=94546241
CallOrigin=1

ChargedUnits=0
InfoType=2
TransmitPackets=6251
TransmitBytes=125020
ReceivePackets=3300
ReceiveBytes=66000
VOIP:
ConnectionId[0x142E62FB 0x5C6705AF 0x0 0x385722B0]
RemoteIPAddress=171.68.235.18

RemoteUDPPort=16580

RoundTripDelay=29 ms

SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
SessionProtocol=cisco
SessionTarget=ipv4:171.68.235.18
OnTimeRvPlayout=63690
GapFillWithSilence=0 ms

GapFillWithPrediction=180 ms

GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=30 ms
ReceiveDelay=40 ms
LostPackets=0 ms

EarlyPackets=1 ms

LatePackets=18 ms

VAD = disabled

CoderTypeRate=g729r8

CodecBytes=20

cvVoIPCallHistoryIcpif=0
SignalingType=cas
```

show call history voice Command Example

The following output is from a Cisco 7200 series router:

```
Router# show call history voice

GENERIC:
SetupTime=94893250 ms
Index=450
PeerAddress=##52258

PeerSubAddress=
PeerId=50000
```

```
PeerIfIndex=35
LogicalIfIndex=0
DisconnectCause=10

DisconnectText=normal call clearing.

ConnectTime=94893780
DisconectTime=95015500
CallOrigin=1

ChargedUnits=0
InfoType=2
TransmitPackets=32258
TransmitBytes=645160
ReceivePackets=20061
ReceiveBytes=401220
VOIP:
ConnectionId[0x142E62FB 0x5C6705B3 0x0 0x388F851C]
RemoteIPAddress=171.68.235.18

RemoteUDPPort=16552

RoundTripDelay=23 ms

SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
SessionProtocol=cisco
SessionTarget=ipv4:171.68.235.18
OnTimeRvPlayout=398000
GapFillWithSilence=0 ms

GapFillWithPrediction=1440 ms

GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=97 ms
LoWaterPlayoutDelay=30 ms
ReceiveDelay=49 ms
LostPackets=1 ms
EarlyPackets=1 ms

LatePackets=132 ms

VAD = disabled

CoderTypeRate=g729r8

CodecBytes=20
cvVoIPCallHistoryIcpif=0
```

Troubleshooting Analog and Digital Voice Port Configurations

7.304

The following sections will assist in analyzing and troubleshooting voice port problems:

- Troubleshooting Chart, page 110
- Voice Port Testing Commands, page 112

Troubleshooting Chart

Table 10 lists some problems you might encounter after configuring voice ports and has some suggested remedies.

Table 10 Troubleshooting Voice Port Configurations

Problem	Suggested Action
No connectivity	Ping the associated IP address to confirm connectivity. If you cannot successfully ping your destination, refer to the *Cisco IOS IP Configuration Guide.*
No connectivity	Enter the **show controller t1** or **show controller e1** command with the controller number for the voice port you are troubleshooting. This will tell you: • If the controller is up. If it is not, use the **no shutdown** command to make it active. • Whether alarms have been reported. • What parameter values have been set for the controller (framing, clock source, line code, cable length). If these values do not match those of the telephony connection you are making, reconfigure the controller. See the "show controller Command Examples" section on page 105 for output.
No connectivity	Enter the **show voice port** command with the voice port number that you are troubleshooting, which will tell you: • If the voice port is up. If it is not, use the **no shutdown** command to make it active. • What parameter values have been set for the voice port, including default values (these do not appear in the output for the **show running-config** command). If these values do not match those of the telephony connection you are making, reconfigure the voice port. See the "show voice port Command Examples" section on page 101 for sample output.
Telephony device buzzes or does not ring	Use the **show voice port** command to confirm that ring frequency is configured correctly. It must match the connected telephony equipment and may be country-dependent.

Table 10 Troubleshooting Voice Port Configurations (continued)

Problem	Suggested Action
Distorted speech	Use the **show voice port** command to confirm the **cptone** keyword setting (also called *region tone*) is US. Setting a wrong cptone could result in faulty voice reproduction during analog-to-digital or digital-to-analog conversions.
Music on hold is not heard	Reduce the music-threshold level.
Background noise is not heard	Enable the **comfort-noise** command.
Long pauses occur in conversation; like speaking on a walkie-talkie	Overall delay is probably excessive; the standard for adequate voice quality is 150 ms one-way transit delay. Measure delay by using ping tests at various times of the day with different network traffic loads. If delay must be reduced, areas to examine include propagation delay of signals between the sending and receiving endpoints, voice encoding delay, and the voice packetization time for various VoIP codecs.
Jerky or choppy speech	Variable delay, or jitter, is being introduced by congestion in the packet network. Two possible remedies are to: • Reduce the amount of congestion in your packet network. Pings between VoIP endpoints will give an idea of the round-trip delay of a link, which should never exceed 300 ms. Network queuing and dropped packets should also be examined. • Increase the size of the jitter buffer with the **playout-delay** command. (See the "Jitter Adjustment" section on page 94.)
Clipped or fuzzy speech	Reduce input gain. (See the "Voice Level Adjustment" section on page 98.)
Clipped speech	Reduce the input level at the listener's router. (See the "Voice Level Adjustment" section on page 98.)
Volume too low or missed DTMF	Increase speaker's output level or listener's input level. (See the "Voice Level Adjustment" section on page 98.)
Echo interval is greater than 25 ms (sounds like a separate voice)	Configure the **echo-cancel enable** command and increase the value for the **echo-cancel coverage** keyword. (See the "Echo Adjustment" section on page 96.)
Too much echo	Reduce the output level at the speaker's voice port. (See the "Voice Level Adjustment" section on page 98.)

Voice Port Testing Commands

These commands allow you to force voice ports into specific states for testing. They require the use of Cisco IOS Release 12.0(7)XK or 12.1(2)T or a later release, and they apply only to Cisco 2600 and 3600 series routers, and to Cisco MC3810 multiservice concentrators. The following types of voice-port tests are covered:

7.302

- Detector-Related Function Tests, page 112
- Loopback Function Tests, page 114
- Tone Injection Tests, page 115
- Relay-Related Function Tests, page 116
- Fax/Voice Mode Tests, page 116

Detector-Related Function Tests

Using the **test voice port detector** command, you are able to force a particular detector into an on or off state, perform tests on the detector, and then return the detector to its original state.

To configure this feature, use the following commands in privileged EXEC mode:

	Command	Purpose

Step 1	**Cisco 2600 and 3600 Series Routers Analog Voice Ports**
	Router# **test voice port** *slot/subunit/port* **detector** {**m-lead** | **battery-reversal** | **loop-current** | **ring** | **tip-ground** | **ring-ground** | **ring-trip**} {**on** | **off**}
	Cisco 2600 and 3600 Series Routers Digital Voice Ports
	Router# **test voice port** *slot/port:ds0-group* **detector** {**m-lead** | **battery-reversal** | **loop-current** | **ring** | **tip-ground** | **ring-ground** | **ring-trip**} {**on** | **off**}
	Cisco MC3810 Multiservice Concentrators Analog Voice Ports
	Router# **test voice port** *slot/port detector* {**m-lead** | **battery-reversal** | **loop-current** | **ring** | **tip-ground** | **ring-ground** | **ring-trip**} {**on** | **off**}
		Identifies the voice port you want to test. Enter a keyword for the detector under test and specify whether to force it to the on or off state.
		Note For each signaling type (E&M, FXO, FXS), only the applicable keywords are displayed. The **disable** keyword is displayed only when a detector is in the forced state.

<table>
<tr><th></th><th>Command</th><th>Purpose</th></tr>
<tr><td></td><td><b>Cisco MC3810 Multiservice Concentrators Digital Voice Ports</b>
<code>Router# test voice port slot:ds0-group detector {m-lead | battery-reversal | loop-current | ring | tip-ground | ring-ground | ring-trip} {on | off}</code></td><td></td></tr>
<tr><td><b>Step 2</b></td><td><b>Cisco 2600 and 3600 Series Routers Analog Voice Ports</b>
<code>Router# test voice port slot/subunit/port detector {m-lead | battery-reversal | loop-current | ring | tip-ground | ring-ground | ring-trip} disable</code>
<b>Cisco 2600 and 3600 Series Routers Digital Voice Ports</b>
<code>Router# test voice port slot/port:ds0-group detector {m-lead | battery-reversal | loop-current | ring | tip-ground | ring-ground | ring-trip} disable</code>
<b>Cisco MC3810 Multiservice Concentrators Analog Voice Ports</b>
<code>Router# test voice port slot/port detector {m-lead | battery-reversal | loop-current | ring | tip-ground | ring-ground | ring-trip} disable</code>
<b>Cisco MC3810 Multiservice Concentrators Digital Voice Ports</b>
<code>Router# test voice port slot:ds0-group detector {m-lead | battery-reversal | loop-current | ring | tip-ground | ring-ground | ring-trip} disable</code></td><td>Identifies the voice port on which you want to end the test. Enter a keyword for the detector under test and the keyword <b>disable</b> to end the forced state.
<b>Note</b> For each signaling type (E&M, FXO, FXS), only the applicable keywords are displayed. The <b>disable</b> keyword is displayed only when a detector is in the forced state.</td></tr>
</table>

7.300

Loopback Function Tests

To establish loopbacks on a voice port, use the following commands in privileged EXEC mode:

<table>
<tr><th></th><th>Command</th><th>Purpose</th></tr>
<tr><td>Step 1</td><td><b>Cisco 2600 and 3600 Series Routers Analog Voice Ports</b>
Router# <b>test voice port</b> <i>slot/subunit/port</i> <b>loopback</b> {<b>local</b> | <b>network</b>}</td><td>Identifies the voice port you want to test and enters a keyword for the loopback direction.
<b>Note</b> A call must be established on the voice port under test.</td></tr>
<tr><td></td><td><b>Cisco 2600 and 3600 Series Routers Digital Voice Ports</b>
Router# <b>test voice port</b> <i>slot/port:ds0-group</i> <b>loopback</b> {<b>local</b> | <b>network</b>}</td><td></td></tr>
<tr><td></td><td><b>Cisco MC3810 Multiservice Concentrators Analog Voice Ports</b>
Router# <b>test voice port</b> <i>slot/port detector</i> <b>loopback</b> {<b>local</b> | <b>network</b>}</td><td></td></tr>
<tr><td></td><td><b>Cisco MC3810 Multiservice Concentrators Digital Voice Ports</b>
Router# <b>test voice port</b> <i>slot:ds0-group</i> <b>loopback</b> {<b>local</b> | <b>network</b>}</td><td></td></tr>
<tr><td>Step 2</td><td><b>Cisco 2600 and 3600 Series Routers Analog Voice Ports</b>
Router# <b>test voice port</b> <i>slot/subunit/port</i> <b>loopback disable</b></td><td>Identifies the voice port on which you want to end the test and enters the keyword disable to end the loopback.</td></tr>
<tr><td></td><td><b>Cisco 2600 and 3600 Series Routers Digital Voice Ports</b>
Router# <b>test voice port</b> <i>slot/port:ds0-group</i> <b>loopback disable</b></td><td></td></tr>
<tr><td></td><td><b>Cisco MC3810 Multiservice Concentrators Analog Voice Ports</b>
Router# <b>test voice port</b> <i>slot/port detector</i> <b>loopback disable</b></td><td></td></tr>
<tr><td></td><td><b>Cisco MC3810 Multiservice Concentrators Digital Voice Ports</b>
Router# <b>test voice port</b> <i>slot:ds0-group</i> <b>loopback disable</b></td><td></td></tr>
</table>

Tone Injection Tests

To inject a test tone into a voice port, use the following commands in privileged EXEC mode:

<table>
<tr><th></th><th>Command</th><th>Purpose</th></tr>
<tr><td><b>Step 1</b></td><td><b>Cisco 2600 and 3600 Series Routers Analog Voice Ports</b>
<code>Router# test voice port <i>slot/subunit/port</i> inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet}</code>
<b>Cisco 2600 and 3600 Series Routers Digital Voice Ports</b>
<code>Router# test voice port <i>slot/port:ds0-group</i> inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet}</code>
<b>Cisco MC3810 Multiservice Concentrators Analog Voice Ports</b>
<code>Router# test voice port <i>slot/port detector</i> inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet}</code>
<b>Cisco MC3810 Multiservice Concentrators Digital Voice Ports</b>
<code>Router# test voice port <i>slot:ds0-group</i> inject-tone {local | network} {1000hz | 2000hz | 200hz | 3000hz | 300hz | 3200hz | 3400hz | 500hz | quiet}</code></td><td>Identifies the voice port you want to test and enter keywords for the direction to send the test tone and for the frequency of the test tone.
<b>Note</b> A call must be established on the voice port under test.</td></tr>
<tr><td><b>Step 2</b></td><td><b>Cisco 2600 and 3600 Series Routers Analog Voice Ports</b>
<code>Router# test voice port <i>slot/subunit/port</i> inject-tone disable</code>
<b>Cisco 2600 and 3600 Series Routers Digital Voice Ports</b>
<code>Router# test voice port <i>slot/port:ds0-group</i> inject-tone disable</code>
<b>Cisco MC3810 Multiservice Concentrators Analog Voice Ports</b>
<code>Router# test voice port <i>slot/port detector</i> inject-tone disable</code>
<b>Cisco MC3810 Multiservice Concentrators Digital Voice Ports</b>
<code>Router# test voice port <i>slot:ds0-group</i> inject-tone disable</code></td><td>Identifies the voice port on which you want to end the test and enter the keyword <b>disable</b> to end the test tone.
<b>Note</b> The <b>disable</b> keyword is available only if a test condition is already activated.</td></tr>
</table>

7.298

Relay-Related Function Tests

To test relay-related functions on a voice port, use the following commands in privileged EXEC mode:

	Command	Purpose

Step 1	**Cisco 2600 and 3600 Series Routers Analog Voice Ports**
	Router# **test voice port** *slot/subunit/port* **relay** {**e-lead** | **loop** | **ring-ground** | **battery-reversal** | **power-denial** | **ring** | **tip-ground**} {**on** | **off**}
	Cisco 2600 and 3600 Series Routers Digital Voice Ports
	Router# **test voice port** *slot/port:ds0-group* **relay** {**e-lead** | **loop** | **ring-ground** | **battery-reversal** | **power-denial** | **ring** | **tip-ground**} {**on** | **off**}
	Cisco MC3810 Multiservice Concentrators Analog Voice Ports
	Router# **test voice port** *slot/port detector* **relay** {**e-lead** | **loop** | **ring-ground** | **battery-reversal** | **power-denial** | **ring** | **tip-ground**} {**on** | **off**}
	Cisco MC3810 Multiservice Concentrators Digital Voice Ports
	Router# **test voice port** *slot:ds0-group* **relay** {**e-lead** | **loop** | **ring-ground** | **battery-reversal** | **power-denial** | **ring** | **tip-ground**} {**on** | **off**}
		Identifies the voice port you want to test. Enter a keyword for the relay under test and specify whether to force it to the on or off state.
		Note For each signaling type (E&M, FXO, FXS), only the applicable keywords are displayed. The **disable** keyword is displayed only when a relay is in the forced state.

Step 2	**Cisco 2600 and 3600 Series Routers Analog Voice Ports** Router# **test voice port** *slot/subunit/port* **relay** {**e-lead** | **loop** | **ring-ground** | **battery-reversal** | **power-denial** | **ring** | **tip-ground**} **disable** **Cisco 2600 and 3600 Series Routers Digital Voice Ports** Router# **test voice port** *slot/port:ds0-group* **relay** {**e-lead** | **loop** | **ring-ground** | **battery-reversal** | **power-denial** | **ring** | **tip-ground**} **disable** **Cisco MC3810 Multiservice Concentrators Analog Voice Ports** Router# **test voice port** *slot/port detector* **relay** {**e-lead** | **loop** | **ring-ground** | **battery-reversal** | **power-denial** | **ring** | **tip-ground**} **disable** **Cisco MC3810 Multiservice Concentrators Digital Voice Ports** Router# **test voice port** *slot:ds0-group* **relay** {**e-lead** | **loop** | **ring-ground** | **battery-reversal** | **power-denial** | **ring** | **tip-ground**} **disable**	Identifies the voice port on which you want to end the test. Enter a keyword for the relay under test, and the keyword **disable** to end the forced state. **Note** For each signaling type (E&M, FXO, FXS), only the applicable keywords are displayed. The **disable** keyword is displayed only when a relay is in the forced state.

Fax/Voice Mode Tests

The **test voice port switch fax** command forces a voice port into fax mode for testing. After you enter this command, you can use the **show voice call** or **show voice call summary** command to check whether the voice port is able to operate in fax mode. If no fax data is detected by the voice port, the voice port remains in fax mode for 30 seconds and then reverts automatically to voice mode.

The **disable** keyword ends the forced mode switch; however, the fax mode ends automatically after 30 seconds. The disable keyword is available only while the voice port is in fax mode.

7.297

To force a voice port into fax mode and return it to voice mode, use the following commands in privileged EXEC mode:

	Command	Purpose

Step 1	**Cisco 2600 and 3600 Series Routers Analog Voice Ports**
	`Router# test voice port slot/subunit/port switch fax`
	Cisco 2600 and 3600 Series Routers Digital Voice Ports
	`Router# test voice port slot/port:ds0-group switch fax`
	Cisco MC3810 Multiservice Concentrators Analog Voice Ports
	`Router# test voice port slot/port detector switch fax`
	Cisco MC3810 Multiservice Concentrators Digital Voice Ports
	`Router# test voice port slot:ds0-group switch fax`
		Identifies the voice port you want to test. Enter the keyword **fax** to force the voice port into fax mode.

Step 2	**Cisco 2600 and 3600 Series Routers Analog Voice Ports**
	`Router# test voice port slot/subunit/port switch disable`
	Cisco 2600 and 3600 Series Routers Digital Voice Ports
	`Router# test voice port slot/port:ds0-group switch disable`
	Cisco MC3810 Multiservice Concentrators Analog Voice Ports
	`Router# test voice port slot/port detector switch disable`
	Cisco MC3810 Multiservice Concentrators Digital Voice Ports
	`Router# test voice port slot:ds0-group switch disable`
		Identifies the voice port on which you want to end the test. Enter the keyword **disable** to return the voice port to voice mode.

AP 6Q

CISCO SYSTEMS

Home | Logged In | Profile | Contacts & Feedback | Site Help

Select a Location / Language

Technical Support

GO

TECHNICAL SUPPORT

SNMP Object Navigator

TECHNICAL SUPPORT

SNMP Object Navigator

Search:

GO

Search All Cisco.com

HOME | TRANSLATE/BROWSE | SEARCH | VIEW & DOWNLOAD MIBS | **MIB SUPPORT IN SOFTWARE**

Toolkit: Roll over tools below

Feedback | Help

Here is a list of MIBs that is supported by c3745-ik9s-mz.12.2-15.T.

CISCO-QLLC01-MIB
CISCO-QUEUE-MIB
CISCO-RSRB-MIB
CISCO-RTTMON-MIB
CISCO-SDLLC-MIB
CISCO-SNAPSHOT-MIB
CISCO-STUN-MIB
CISCO-SYSLOG-MIB
CISCO-TCP-MIB
CISCO-VOICE-ANALOG-IF-MIB
CISCO-VOICE-COMMON-DIAL-CONTROL-MIB
CISCO-VOICE-ENABLED-LINK-MIB
CISCO-VOICE-FR-DIAL-CONTROL-MIB
CISCO-VPDN-MGMT-EXT-MIB
ETHERLIKE-MIB
EVENT-MIB
IMA-MIB
MSDP-MIB
XGCP-MIB
CISCO-IPSEC-FLOW-MONITOR-MIB
CISCO-VOICE-DIAL-CONTROL-MIB
CISCO-VOICE-IF-MIB
CISCO-VPDN-MGMT-MIB
DIAL-CONTROL-MIB
DLSW-MIB
ENTITY-MIB
EXPRESSION-MIB
HC-RMON-MIB
IF-MIB
INT-SERV-GUARANTEED-MIB
IGMP-STD-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB
SNMP-NOTIFICATION-MIB
IP-FORWARD-MIB
CISCO-ENTITY-ASSET-MIB
CISCO-IPSEC-MIB
CISCO-SIP-UA-MIB
CISCO-IPSEC-POLICY-MAP-MIB
CISCO-MOBILE-IP-MIB
CISCO-PIM-MIB
CISCO-SAA-APM-MIB
CISCO-PRODUCTS-MIB
CISCO-BGP4-MIB
CISCO-IETF-NAT-MIB
CISCO-PPPOE-MIB
MIP-MIB
CISCO-ATM-PVCTRAP-EXTN-MIB
CISCO-IETF-IP-FORWARD-MIB

Related Tools

TAC Case Open
TAC Case Query
MIB Locator

7.204
k

CISCO-IETF-IP-MIB
IPMROUTE-STD-MIB
INT-SERV-MIB
ISDN-MIB
LAN-EMULATION-CLIENT-MIB
OLD-CISCO-CHASSIS-MIB
OLD-CISCO-CPU-MIB
OLD-CISCO-INTERFACES-MIB
OLD-CISCO-IP-MIB
OLD-CISCO-MEMORY-MIB
OLD-CISCO-SYSTEM-MIB
OLD-CISCO-TCP-MIB
OLD-CISCO-TS-MIB
PIM-MIB
RFC1213-MIB
RFC1231-MIB
RFC1253-MIB
RFC1315-MIB
RFC1381-MIB
RFC1382-MIB
RFC1406-MIB
RFC1407-MIB
ATM-MIB
BGP4-MIB
BRIDGE-MIB
CISCO-ACCESS-ENVMON-MIB
CISCO-ALPS-MIB
CISCO-ATM-EXT-MIB
CISCO-BSC-MIB
CISCO-BSTUN-MIB
CISCO-BULK-FILE-MIB
RFC1595-MIB
CISCO-BUS-MIB
RMON-MIB
RMON2-MIB
RS-232-MIB
RSVP-MIB
SMON-MIB
SNA-SDLC-MIB
SNMP-FRAMEWORK-MIB
SNMP-TARGET-MIB
SNMP-USM-MIB
CISCO-CALL-HISTORY-MIB
CISCO-CAR-MIB
CISCO-CDP-MIB
CISCO-COMPRESSION-SERVICE-ADAPTER-MIB
CISCO-CONFIG-COPY-MIB
CISCO-CONFIG-MAN-MIB
CISCO-DIAL-CONTROL-MIB
CISCO-DLCSW-MIB
CISCO-DLSW-EXT-MIB
CISCO-DLSW-MIB
CISCO-DSPU-MIB
CISCO-ENVMON-MIB
CISCO-FLASH-MIB
CISCO-FRAME-RELAY-MIB
CISCO-FTP-CLIENT-MIB
CISCO-H323-TC-MIB
CISCO-HSRP-EXT-MIB
CISCO-HSRP-MIB
CISCO-IETF-ATM2-PVCTRAP-MIB
CISCO-IMAGE-MIB
SNMP-VACM-MIB
SNMPv2-MIB
SOURCE-ROUTING-MIB
TCP-MIB
UDP-MIB
OLD-CISCO-FLASH-MIB

CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
CISCO-VLAN-MEMBERSHIP-MIB
CISCO-VTP-MIB
CISCO-CLASS-BASED-QOS-MIB
CISCO-IP-STAT-MIB
CISCO-IPMROUTE-MIB
CISCO-ISDN-MIB
CISCO-LEC-DATA-VCC-MIB
CISCO-LEC-EXT-MIB
CISCO-LECS-MIB
CISCO-LES-MIB
CISCO-MEMORY-POOL-MIB
CISCO-PING-MIB
CISCO-PROCESS-MIB
CISCO-ICSUDSU-MIB
CISCO-ISDNU-IF-MIB
CISCO-STACKMAKER-MIB
CISCO-POP-MGMT-MIB
CISCO-CALL-APPLICATION-MIB
CISCO-CAS-IF-MIB
CISCO-CIRCUIT-INTERFACE-MIB
CISCO-DSP-MGMT-MIB
CISCO-NTP-MIB
CISCO-VOICE-ATM-DIAL-CONTROL-MIB

BUSINESS INDUSTRIES & SOLUTIONS | NETWORKING SOLUTIONS & PROVISIONED SERVICES | PRODUCTS & SERVICE
TECHNOLOGIES | ORDERING | TECHNICAL SUPPORT | LEARNING & EVENTS | PARTNERS & RESELLERS | ABOUT CISCO
Home | Logged In | Profile | Contacts & Feedback | Site Help